$N°$d'ordre : 2589

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par David MASSON

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

****

FONCTIONS HARMONIQUES, CODES ET DESIGNS

****

Soutenue le : 22 novembre 2002

Après avis de :

MM.	E. Bannai	Professeur	Université de Kyushu	**Rapporteurs**
	P. Solé	Directeur de recherches	Université de Sophia-Antipolis	

Devant la commission d'examen formée de :

MM.	P. Solé	Directeur de recherches	Université de Sophia-Antipolis	**Président**
	P. Gaborit	Maître de conférences	Université de Limoges	**Rapporteur**
	C. Bachoc	Professeur	Université de Bordeaux 1	**Examinateurs**
	G. Kabatianski	Professeur	Université de de Moscou	
	A. Zvonkine	Professeur	Université de Bordeaux 1	

- 2002 -

Remerciements

Tout d'abord je tiens à remercier Christine Bachoc, ma directrice de thèse, pour sa grande disponibilité, pour ses multiples conseils et remarques, pour la qualité de son encadrement enfin sans lesquels cette thèse n'aurait probablement pas vu le jour.

Eiichi Bannai et Patrick Solé ont bien voulu accepter de rapporter le présent mémoire. En outre ils m'ont beaucoup appris à chaque fois que j'ai pu avoir l'occasion de les rencontrer, me faisant profiter de leur expérience et de leurs idées. Je leur suis par conséquent extrêmement reconnaissant.

Mes remerciements s'adressent également à Philippe Gaborit, Grigori Kabatianski et Alexandre Zvonkine qui, en acceptant d'être membre de mon jury, ont manifesté de l'intérêt à l'égard de mes travaux.

Alors que j'étais en DEA je suis resté longtemps indécis quant au sujet de mon mémoire, lequel allait déterminer l'orientation de ma thèse. C'est grâce à Jacques Martinet que je me suis finalement engagé dans la voie que j'ai depuis lors suivie et il va sans dire que sans lui la présente thèse n'aurait jamais vu le jour. Je lui adresse par conséquent, à lui aussi, toute ma gratitude.

J'ai eu la chance d'effectuer ma thèse dans d'excellentes conditions au sein du laboratoire A2X, et je profite donc de l'occasion qui m'est offerte ici pour en remercier tous les membres et plus particulièrement son directeur, Michel Olivier.

Véronique Saint-Martin et Maud Besson, nos secrétaires, ainsi que Mauricette Jaubert, responsable des travaux d'imprimerie, ont toujours fait preuve d'une grande serviabilité et d'un grand sérieux pour les multiples tâches que j'ai pu leur confier. Aussi je tiens à ce qu'elles sachent combien je leur en suis reconnaissant.

Enfin je tiens à exprimer ma plus sincère amitié à toutes celles et tous ceux, collègues et amis, avec qui j'ai eu l'occasion de passer de bons moments au cours de ces dernières années. En particulier je n'oublierai jamais les heures de conversation passées avec Sami Omar, qui travaillait dans le même bureau que moi : c'est en effet probablement dans ces moments-là que j'ai le plus appris...

Merci à tous,
David.

Table des matières

Introduction

Au cours des trois années qu'a duré cette thèse nous nous sommes d'abord intéressés aux *designs* et aux *schémas d'association*.

Schémas d'association

Formellement, un schéma d'association (SA en abrégé) est un ensemble fini muni de relations d'équivalence vérifiant la propriété suivante : le $\mathbb{C}$-espace vectoriel engendré par les matrices de ces relations est une $\mathbb{C}$-algèbre commutative, stable par conjugaison (rappelons que la matrice $\mathcal{M}$ d'une relation $\mathcal{R}$ sur un ensemble fini $X = \{x_1, \ldots, x_n\}$ est indexée sur $X \times X$ et est définie par $M_{x,y} = 1$ ou 0 selon que $x\mathcal{R}y$ ou non).
Lorsqu'on étudie des objets de nature combinatoire, il peut être intéressant de les plonger dans un SA (bien choisi) car ces derniers présentent une structure riche, et l'on dispose alors de nombreux outils. Ainsi P. Delsarte a montré que les SA offraient un cadre naturel pour la théorie des codes et celle des designs, unifiant les deux théories en les rendant duales l'une de l'autre ([7]). D'abord étudiés en statistiques (sous forme de PBD) par R.C. Bose et ses collègues dans les années 50, puis en théorie des groupes par D.G. Higman (en 1971), les SA acquièrent à nouveau de l'importance en 1973, dans la thèse de P. Delsarte : d'une part sur le plan théorique puisqu'ils fournissent un important concept unificateur de la combinatoire (algébrique), d'autre part sur le plan pratique puisque grâce à la méthode de programmation linéaire ils permettent d'encadrer taille de codes et de designs.

Designs

La théorie des designs, quant à elle, tire son nom de la Statistique : en anglais, *design of experiments* signifie *élaboration d'expériences*. Donnons un exemple historique ([11],[13]) ; supposons que l'on cherche à tester v variétés d'engrais : une méthode consiste à appliquer ces différents traitements à un champ partagé en v parcelles, l'engrais choisi étant bien sûr celui qui donne

le meilleur rendement. Toutefois la fertilité d'un sol pouvant beaucoup varier au sein d'un même champ, on ne peut garantir la fiabilité de cette méthode. Pour résoudre ce problème, R. A. Fisher (1890-1962), éminent statisticien du vingtième siècle, eut l'idée suivante ([11]) : partager chacune des parcelles en k parties sur lesquelles on appliquera les différents traitements (les parcelles ne sont plus nécessairement au nombre de v). Pour avoir de bons résultats, il est préférable que chaque paire possible de traitements apparaisse le même nombre de fois dans les diverse parcelles, disons λ fois. Dès lors on s'affranchit (en moyenne) de l'hétérogénéité du sol. Comme on peut l'imaginer, de nombreux problèmes d'optimisation (dans l'industrie par exemple) se ramènent à des situations similaires ([13]). Ils ont donné lieu à la théorie (mathématique) des designs.

De façon générale, si X est un ensemble fini (de *points*) et $\mathcal{B}$ une famille de parties (appelées *blocs*) de X, un design est un couple $(X, \mathcal{B})$ vérifiant certaines propriétés de régularité. Plus précisément, $(X, \mathcal{B})$ est un t-(v, k, λ) *design* ou encore un *t-design combinatoire* si :

- $|X| = v$,
- les blocs de $\mathcal{B}$ sont tous de taille k (i.e. de cardinal k),
- toute partie de X à t éléments est contenue dans exactement λ blocs.

Ainsi, dans l'exemple précédent, Fisher travaille avec un 2-(v, k, λ) design (de tels designs sont souvents appelés *BIBD*, de l'anglais : *Balanced Incomplete Block Designs*). On peut montrer facilement qu'un t-design combinatoire est un i-design combinatoire pour tout $i \leq t$. Ainsi tout point apparaît le même nombre de fois dans l'ensemble des blocs. Ce nombre est noté r. Toujours dans notre exemple, r correspond au nombre de fois qu'un engrais a été testé (on utilise r pour *replication* et v pour *varieties* ; ces notations sont restées d'usage depuis). Si l'on note $b = |\mathcal{B}|$ le nombre de blocs, on a la célèbre inégalité de Fisher : $b \geq v$ (pour $1 < k < v$). Elle montre qu'il faut toujours au moins autant de parcelles que d'engrais à tester. Par ailleurs on peut montrer que : $vr = bk$. L'inégalité de Fisher s'écrit donc aussi : $r \geq k$.

De façon générale r correspond au nombre de fois qu'une certaine expérience est identiquement reproduite. Or faire des répliques peut, selon les cas, coûter de l'argent, demander du temps ou encore être source d'erreurs. C'est pourquoi l'on a étudié des designs qui échapperaient à l'inégalité de Fisher. Ainsi furent introduits les *PBD* (de l'anglais : *Partially Balanced Designs*). En fait, les schémas d'association apparurent en statistiques, en même temps que les PBD ; en effet la définition même des PBD nécessite la présence d'une structure particulière, à savoir celle de schéma d'association.

Représentation du groupe symétrique

Nous ferons au chapitre 3 des rappels sur la théorie des SA et nous indiquerons notamment comment cette théorie est étroitement liée à la représentation des groupes, via certaines fonctions *harmoniques* (c'est-à-dire *zonales sphériques*, cf. troisième partie). C'est pourquoi nous avons préféré commencer notre exposé par des rappels sur la représentation du groupe qui, en ce qui nous concerne, interviendra naturellement : le groupe symétrique.
Les représentations irréductibles de ce groupe sont bien connues depuis les travaux de Frobenius et surtout d'Alfred Young (cf. [28]). Nous ferons dans le premier chapitre quelques rappels sur leur description explicite et nous utiliserons pour cela la décomposition classique :

$$\mathbb{C}[X_s] \simeq \mathrm{Ind}_{S_s}^{S_n} 1 \simeq \bigoplus_{\lambda \trianglerighteq s} K_{\lambda s}[\lambda]$$

où $S_s \simeq S_{s_1} \times \ldots \times S_{s_q}$ est le *sous-groupe de Young* associé à la partition $s = (s_1, \ldots, s_q)$ de l'entier n, X_s est l'ensemble des mots $q - aires$ de composition s et où les $K_{\lambda s}$ sont les *nombres de Kotska*.
En revanche nous n'avons pu trouver nulle part de formules pour calculer les fonctions harmoniques associées à cette décomposition. Aussi les expliciterons-nous au chapitre 2 (théorème 10, cf. aussi théorème 3 de [19]).
Au chapitre 4, après quelques rappels sur les designs nous en étudierons une récente généralisation due à A. Bonnecaze, E. Rains et P. Solé ([2]) : les *designs colorés* (au sens fort). Plus précisément nous montrerons (theorème 21, cf. aussi théorème 2 de [19]) comment cette notion s'insère dans la théorie des schémas d'association et nous établirons, grâce aux fonctions harmoniques du chapitre 2, un algorithme pour tester si un ensemble est (ou n'est pas) un design généralisé.

Codes

La dernière partie de cette thèse concerne les codes.
Rappelons brièvement la problématique qui sous-tend la théorie des codes correcteurs d'erreurs. Lorsque l'on effectue une transmission d'information ([16]) on n'envoie jamais parfaitement un message : si celui-ci correspond à une chaîne de 0 et de 1 (ou, plus généralement, à des éléments du corps fini $\mathbb{F}_q$), au cours de la transmission certains des 0 peuvent se transformer en 1 et *vice versa*. On pallie cet inconvénient en n'utilisant que certaines chaînes (qu'on appelle aussi *mots* ; leur *poids* est le nombre de leurs coordonnées non nulles). Un code sera alors l'ensemble des mots admissibles. Par exemple, si l'on envoie des mots binaires de longueur 3 et si l'on n'autorise que les mots

$(0,0,0)$ et $(1,1,1)$, on est en mesure de faire de la détection et de la correction d'erreurs. En effet, si l'on reçoit le mot $(0,1,0)$ on sait qu'une erreur s'est produite et qu'à l'origine le mot envoyé était probablement $(0,0,0)$ car il ne diffère que d'un terme de $(0,1,0)$ tandis que $(1,1,1)$ en diffère de deux. On définit ainsi la *distance* entre deux mots comme étant le poids de leur différence et la *distance minimale* d'un code comme la plus petite distance existant entre deux de ses mots. Bien sûr, le problème est de trouver des codes ayant beaucoup de mots tout en ayant une distance minimale assez grande. D'où une notion *d'extrémalité* que nous rappellerons au chapitre 5, après quelques rappels généraux sur la théorie des codes. On se rend compte alors que les bons codes (c'est-à-dire les codes extrémaux) ont tendance à contenir de bons designs (théorème d'Assmus-Mattson). Nous utiliserons l'algorithme déduit du théorème 21 pour voir à travers quelques exemples ce qu'il en est pour les codes non-binaires et les designs généralisés (i.e. les designs colorés au sens fort de [2]).

Invariants des groupes de Clifford

Par ailleurs, les codes jouent également un rôle important dans la théorie des réseaux ([10]) : appelons code linéaire C, tout sous-espace vectoriel de $\mathbb{F}_p^n$ (p premier). L'image réciproque de C par la surjection canonique : $\mathbb{Z}^n \to (\mathbb{Z}/p\mathbb{Z})^n$ est un réseau noté L_C ; beaucoup de propriétés intéressantes de C (parité, autodualité, ...) se traduisent par des propriétés intéressantes sur L_C (réseau pair, unimodulaire, ...). De plus on dispose de critères pour savoir si un réseau provient d'un code ou non. Il y a en fait une espèce de dualité entre théorie des codes et théorie des réseaux. En particulier, de même que l'on sait associer à un réseau une forme modulaire (sa série *thêta*) on sait associer à un code un polynôme - son énumérateur de poids - invariant pour l'action d'un certain groupe (le groupe de Clifford).
Ces résultats peuvent être généralisés : on peut associer à un réseau une série thêta multiple ou une série thêta à coefficients sphériques (cf. [10]). Ce sont des formes modulaires et, de plus, la seconde peut être obtenue à partir de la première grâce à un certain opérateur différentiel (cf. [12]). Or, C. Bachoc a pu définir pour un code binaire des *énumérateurs de poids harmoniques* (cf. [1]) pour lesquels elle a montré des résultats d'invariance sous l'action du groupe de Clifford. En outre on peut montrer des résultats d'invariance pour des *énumérateurs de poids multiple*. Enfin dans [21] M. Ozeki définit des *polynômes de Jacobi* pour lesquels il montre également des résultats d'invariance.
Nous définirons au chapitre 6 des *énumérateurs de Jacobi multiples* (défini-

Première partie

Fonctions harmoniques du groupe symétrique

Chapitre 1

Représentation du groupe symétrique

Dans ce chapitre nous rappelons sans preuve des résultats classiques sur les représentations (irréductibles, explicites) du groupe symétrique. Cela nous pemet de mettre en place toutes les notations relatives aux tableaux dont nous aurons besoin par la suite. Pour plus de détails sur la représentration du groupe symétrique nous renvoyons le lecteur à [25] (très facile à lire) ou à [15] (très complet).

1.1 Généralités

Soit G un groupe fini et soit V un espace vectoriel sur le corps $\mathbb{C}$ des nombres complexes. On note $Gl(V)$ le groupe des isomorphismes de V sur lui-même.

Définition 1 *Une représentation de G dans V est un homomorphisme ρ du groupe G dans le groupe $Gl(V)$.*

On dit souvent pour simplifier une "représentation V". On dit que deux représentations $\rho : G \to Gl(V), \rho' : G \to Gl(V')$ sont isomorphes s'il existe un isomorphisme $f : V \to V'$ tel que :

$$f \circ \rho(g) = \rho(g) \circ f \quad \forall g \in G.$$

Une *sous-représentation* de V est un sous-espace vectoriel de V stable pour l'action de G.
Soit $\rho : G \to Gl(V)$ une représentation de G dans V. On dit qu'elle est irréductible si V n'est pas réduit à $\{0\}$ et si aucun sous-espace vectoriel de

V n'est stable pour l'action de G, à part bien entendu $\{0\}$ et V.
Deux éléments g et g' de G sont dits *conjugués* s'il existe $h \in G$ tel que $g' = hgh^{-1}$; c'est là une relation d'équivalence qui partage G en *classes* dites de *conjugaison*.

Théorème 1 *Si G est un groupe fini, le nombre des représentations irréductibles de G (à isomorphisme près) est fini, égal en fait au nombre des classes de conjugaison de G.*

Toute représentation V est somme directe de représentations irréductibles $V = \bigoplus_W m_W W$: dans cette écriture on a groupé les sous-représentations isomorphes et on a noté leur somme directe $m_W W$, m_W étant le nombre de représentations isomorphes à W. Une telle décomposition est unique ; par ailleurs l'entier m_W s'appelle la *multiplicité* de W.

Caractères

Définition 2 *Soit $\rho : G \to Gl(V)$ une représentation de G dans V. Pour tout $g \in G$ posons :*

$$\chi_\rho(g) = Tr(\rho(g)).$$

La fonction $\chi_\rho : G \to \mathbb{C}$ ainsi obtenue s'appelle le caractère de la représentation ρ.

Remarque : dans cette définition Tr désigne la trace, c'est-à-dire la somme des valeurs propres, de l'opérateur linéaire $\rho(g)$.
Comme leur nom l'indique, les caractères *caractérisent* la représentation dont ils proviennent : en effet, deux représentations de même caractère sont isomorphes.
Par ailleurs les caractères vérifient d'importantes relations d'orthogonalité. Soient ϕ, ψ deux fonctions à valeurs complexes, définies sur le groupe G ; posons :

$$< \phi, \psi >_G = |G|^{-1} \sum_{g \in G} \overline{\phi(g)}\, \psi(g).$$

On a alors les résultat suivants :

Théorème 2 *Si χ est le caractère d'une représentation irréductible de G on a : $< \chi, \chi >_G = 1$.*
Si χ et χ' sont les caractères de deux représentations irréductibles de G non isomorphes on a : $< \chi, \chi' >_G = 0$.
Si V est une représentation de G de caractère ϕ et si W est une représentation irréductible de G de caractère χ, on a : $< \phi, \chi >_G = m_W$, multiplicité éventuellemnt nulle de W dans la décomposition de V.

Terminons ces rappels avec la notion de *représentation induite.*
Soient H un sous-groupe de G, $W \subset V$ deux espaces vectoriels, tels que H opère sur W et G sur V.

Définition 3 *On dit que la représentation V de G est induite par la représentation W de H si les conditions suivantes sont réalisées :*
- *W est un sous-module de V, considéré comme $\mathbb{C}[H]$-module à gauche,*
- *$V = \sum_{g \in G/H} gW$.*

Il existe une et une seule représentation de G (à isomorphisme près) induite par une représentation donnée ρ_H de H.
On la note $\mathrm{Ind}_H^G\ \rho_H$.
Soit n un entier, on note S_n le *groupe symétrique* formé des *permutations* de l'ensemble $\{1, 2, \ldots, n\}$. Dorénavant G sera le groupe symétrique S_n.

Classes de conjugaison de S_n

Comme on l'a vu dans la précédente section le nombre des représentations irréductibles de G est égal au nombre des classes de conjugaison de G. Nous allons préciser ce nombre.
Etant donné une permutation $\sigma \in S_n$ elle admet une unique décomposition en un produit (commutatif) de *cycles disjoints* : $\sigma = c_1 \ldots c_k$. La *longueur* d'un cycle $c = (a, \sigma(a), \ldots, \sigma^r(a))$ est par définition l'entier $r+1$. Si l'on conjugue σ avec une autre pertmutation τ, on peut écrire : $\tau\sigma\tau^{-1} = \tau c_1 \tau^{-1} \ldots \tau c_k \tau^{-1}$ et l'on voit donc que le nombre de cycles ainsi que leur longueur respective sont conservés puisque le conjugué $\tau c \tau^{-1}$ d'un cycle est un cycle de même longueur. Associons à une permutation la suite des longueurs des cycles qui la composent, rangées dans l'ordre décroissant, nous obtenons une suite décroissante d'entiers ultimement nulle et dont la somme des termes est n ; une telle suite s'appelle une *partition* de l'entier n. Ainsi deux permutations sont-elles conjuguées si et seulement si les partitions associées à leur décomposition en cycles disjoints sont égales. On en déduit donc :

Théorème 3 *Il y a autant de S_n modules irréductibles que de partitions de l'entier n.*

Dans la suite de ce chapitre nous construirons une bijection explicite entre partitions de n et S_n modules irréductibles.

1.2 Mots, tableaux et tabloïdes

Tableaux

A une partition $\lambda = (\lambda_1, \ldots, \lambda_l)$ on associe son *diagramme de Ferrers*, formé de croix que l'on range en lignes ; plus précisément la $i^{ième}$ ligne est formée de λ_i croix.
Exemple : pour $n = 12,\ \lambda = (4, 3, 3, 2)$, le diagramme de λ est :

$$\begin{array}{l} \times\times\times\times \\ \times\times\times \\ \times\times\times \\ \times\times \end{array}$$

A partir de ce diagramme on en construit un second en transposant lignes et colonnes. On note λ^* la partition de n associée à ce nouveau diagramme. Avec l'exemple précédent on obtient :

$$\begin{array}{l} \times\times\times\times \\ \times\times\times\times \\ \times\times\times \\ \times \end{array}$$

et $\lambda^* = (4, 4, 3, 1)$.

Définition 4 *En remplaçant les croix du diagramme de λ par des entiers on obtient un tableau généralisé de type λ.*

Exemple précédent :

$$t = \begin{array}{l} 1182 \\ 231 \\ 641 \\ 11 \end{array}$$

Soit s_i le nombre de i dans un tableau généralisé. La *composition* de ce tableau est par définition la suite $s = (s_1, \ldots, s_m, \ldots)$. En principe nous devrions rajouter s_0 mais en pratique les coefficients des tableaux généralisés sont toujours non nuls. La suite est bien évidemment ultimement nulle. Aussi en pratique l'écrit-on comme un m-uplet, m étant le plus grand coefficient du tableau. Ainsi la composition du tableau généralisé de l'exemple précédent est : $(6, 2, 1, 1, 0, 1, 0, 1)$. On note $T_{\lambda s}$ l'ensemble des tableaux généralisés de type λ et de composition s.

Définition 5 *Un tableau généralisé est dit semi-standard si ses lignes croissent et si ses colonnes croissent strictement.*

Exemple :

$$t = \begin{array}{l} 1335 \\ 25 \\ 7 \end{array}$$

On note $T'_{\lambda s}$ l'ensemble des tableaux généralisés semi-standards de type λ et de composition s.

Définition 6 *Un tableau généralisé dont la composition est* $(\underbrace{1, 1, \ldots, 1}_{q}, 0, 0, \ldots)$ *est appelé tableau.*

Autrement dit un tableau est un tableau généralisé formé de tous les entiers de 1 à q.
Exemple :

$$t = \begin{array}{l} 526 \\ 13 \\ 4 \end{array}$$

On note T_λ l'ensemble des tableaux de type λ.

Définition 7 *Un tableau est dit standard si ses lignes et ses colonnes croissent.*

Cette définition est bien sûr un cas particulier de la définition 5 puisque un tableau semi-standard est la même chose qu'un tableau standard, tous ses coefficients étant distincts.
Exemple :

$$t = \begin{array}{l} 135 \\ 24 \\ 6 \end{array}$$

On note T'_λ l'ensemble des tableaux standards de type λ.

Tabloïdes

On definit une relation d'équivalence $\sim$ sur $T_{\lambda s}$: $t' \sim t$ signifie que les lignes de t' et t sont les mêmes à l'ordre près de leurs termes.

Exemple : $t = \begin{array}{l} 112 \\ 23 \end{array}$ les tableaux t' tels que $t' \sim t$ sont :

$$\begin{array}{lllllll} 112 & 121 & 211 & 112 & 121 & 211 \\ 23 \ , & 23 \ , & 23 \ , & 32 \ , & 32 \ , & 32 \end{array}$$

Soit $t \in T_{\lambda s}$ on note $\overline{t}$ sa classe d'équivalence pour la relation $\sim$. En faisant de même pour les lignes de t on obtient une écriture commode de $\overline{t}$ à partir d'un de ses représentants.
Exemple : $t = \begin{matrix} 112 \\ 23 \end{matrix}$, $\overline{t} = \begin{matrix} \overline{112} \\ \overline{23} \end{matrix}$

Définition 8 *On note $\mathcal{T}_{\lambda s}$ le quotient $T_{\lambda s}/\sim$; ses éléments sont appelés tabloïdes généralisés de type λ et de composition s.*

Définition 9 *On note $\mathcal{T}_\lambda$ le quotient $T_\lambda/\sim$; ses éléments sont appelés tabloïdes de type λ.*

Mots

Les tabloïdes introduits dans le paragraphe précédent permettent de décrire explicitement les S_n modules irréductibles (cf. paragraphe 1.3). Toutefois leur construction peut sembler quelque peu artificielle ; il n'en est rien car ils correspondent en fait à des objets tout à fait familiers comme on s'en rendra compte en lisant ce qui suit.
Soit q un entier et soit $\mathcal{F}_q$ un *alphabet* (c'est-à-dire un ensemble) à q éléments : $\mathcal{F}_q = \{a_1, \ldots, a_q\}$. Pour alléger les notations nous prendrons dorénavant $\mathcal{F}_q = \{1, \ldots, q\}$. Les éléments de l'ensemble $X \overset{déf}{=} \mathcal{F}_q^n$ sont appelés *mots q-aires* et sont dits de *longueur* n. La *composition* d'un tel mot est le q-uplet $s = (s_1, \ldots, s_q)$ où s_i est le nombre de i du mot.
Exemple : $n = 5,\ q = 3,\ x = (1, 1, 2, 1, 3),\ s(x) = (3, 1, 1)$.
On note X_s l'ensemble des mots de même composition s ; on peut toujours supposer que s est une partition, quitte à réindexer l'ensemble $\mathcal{F}_q = \{a_1, \ldots, a_q\}$. Maintenant, si l'on y regarde de plus près, on se rend compte qu'il y a un lien étroit entre X_s et les tabloïdes de type s : en effet, associons à tout élément $\overline{t}$ de $\mathcal{T}_s$ le mot de X_s dont les termes égaux à i ont pour coordonnées les éléments de la $i^{ième}$ ligne de $\overline{t}$. On se rend alors facilement compte que cette association est en fait une *bijection*.
Exemple : $\overline{t} = \begin{matrix} \overline{124} \\ \overline{3} \\ \overline{5} \end{matrix} \quad \rightarrow (1, 1, 2, 1, 3)$.
Par ailleurs on peut également faire correspondre tableaux généralisés et mots de même composition, et cela quelque soit le type du tableau : il suffit en effet d'écrire ce dernier sur une seule ligne.
Exemple : $s = (3, 1, 1),\ t = \begin{matrix} 11 \\ 21 \\ 3 \end{matrix} \rightarrow (1, 1, 2, 1, 3)$.

D'où les bijection suivantes pour toute partition λ :

$$T_{\lambda s} \xrightarrow{\sim} X_s \xrightarrow{\sim} \mathcal{T}_s$$

1.3 Modules de Specht

Action du groupe symétrique

Le groupe symétrique S_n agit sur $T_{\lambda s}$ en permutant ses n coordonnées (numérotées de gauche à droite en partant d'en haut). Exemple : $(1,2,5)$ $\begin{matrix}342\\21\\5\end{matrix}$ $=$ $\begin{matrix}132\\24\\5\end{matrix}$

Dans le cas de T_λ on peut faire agir S_n d'une autre façon : en effet les *coefficients* $t \in T_\lambda$ correspondent exactement à l'ensemble $\{1,2,\ldots,n\}$ d'où l'idée de les permuter : $(1,2,5)$ $\begin{matrix}342\\61\\5\end{matrix}$ $=$ $\begin{matrix}345\\62\\1\end{matrix}$

Pour éviter toute ambiguité dans le cas de T_λ nous appellerons la première action *action sur les coordonnées*, et la seconde *action sur les coefficients*. En revanche S_n ne peut agir que sur les coefficients des tabloïdes car seule cette action passe au quotient.

Exemple : $(1,2,5)$ $\begin{matrix}\overline{342}\\\overline{61}\\\overline{5}\end{matrix}$ $=$ $\begin{matrix}\overline{345}\\\overline{62}\\\overline{1}\end{matrix}$

Polytabloïdes

Soit $\mathcal{E} = \{e_1,\ldots,e_k\}$ un ensemble fini ; on note $\mathbb{C}[\mathcal{E}]$ l'espace vectoriel sur $\mathbb{C}$ engendré formellement par les éléments de $\mathcal{E}$:

$$\mathbb{C}[\mathcal{E}] = \bigoplus_{e\in\mathcal{E}} \mathbb{C}e.$$

Si G agit sur $\mathcal{E}$ alors $\mathbb{C}[\mathcal{E}]$ est bien sûr un G-module. Dans la section précédente nous avons donné quelques exemples d'ensembles sur lesquels le groupe symétrique agissait. Nous allons utiliser l'un d'eux - les tabloïdes en fait - pour décrire explicitement les S_n modules irréductibles.
Soit $\lambda = (\lambda_1,\ldots,\lambda_l)$ une partition de l'entier n et soit t un tableau de type λ : les coefficients de ses colonnes forment une partition de $\{1,2,\ldots,n\}$. On

note $C(t)$ le stabilisateur dans S_n de cette partition.
Exemple : $C\begin{pmatrix} 341 \\ 25 \\ 6 \end{pmatrix} = S_{\{3,2,6\}} \times S_{\{4,5\}} \times S_{\{1\}}$

Définition 10 *Soit t un tableau de type λ on appelle polytabloïde associé à t l'élément de $\mathbb{C}[\mathcal{T}_\lambda]$ défini par :*

$$e_t = \sum_{\sigma \in C(t)} \varepsilon(\sigma)\sigma\overline{t}$$

Remarque : dans cette définition ε désigne la *signature* de la permutation σ ; quant à l'action de cette permutation sur $\overline{t}$ elle ne peut se faire bien sûr que sur ses *coefficients* (cf. 1.3).
Nous sommes maintenant enfin en mesure d'exhiber les représentations irréductibles de S_n.

Définition 11 *Soit λ une partition de n, on appelle module de Specht associé à λ et on note $[\lambda]$ le sous-module de $\mathbb{C}[\mathcal{T}_\lambda]$ défini par :*

$$[\lambda] = Vect\{e_t, t \in T_\lambda\}$$

Théorème 4 *Les modules de Specht forment une liste complète de S_n modules irréductibles.*

On connaît en fait une base de $[\lambda]$:

Théorème 5 *La famille de polytabloïdes $\{e_t, t \in T'_\lambda\}$ est une base de $[\lambda]$. Ainsi on a :*

$$dim[\lambda] = |T'_\lambda|$$

1.4 L'espace $\mathbb{C}[X_s]$

Décomposition de $\mathbb{C}[X_s]$

Soit $s = (s_1, \ldots, s_q)$ une partition de l'entier n. L'espace X_s a été défini au paragraphe 1.2 comme l'ensemble des mots de $X = (\mathcal{F}_q)^n$ de composition s. On notera x_s le mot de composition s qui est de la forme :

$$x_s = (\underbrace{1, \ldots, 1}_{s_1}, \underbrace{2, \ldots, 2}_{s_2}, \ldots, \underbrace{q, \ldots, q}_{s_q})$$

On appelle *sous-groupe de Young* associé à s le stabilisateur dans S_n de x_s :

$$S_s \simeq S_{s_1} \times \ldots \times S_{s_q}$$

Nous avons donc : $X_s \simeq S_n/S_s$. On en déduit :

$$\mathbb{C}[X_s] \simeq \mathrm{Ind}_{S_s}^{S_n} 1$$

or on sait décomposer cette représentation : introduisons au préalable pour cela une relation d'ordre sur les partitions.
Soit $s = (s_1, \ldots, s_q)$ et $\lambda = (\lambda_1, \ldots, \lambda_l)$ deux partitions, on dit que λ *domine* s et on note $\lambda \trianglerighteq s$ si l'on a :

$$\lambda_1 + \ldots + \lambda_i \geq s_1 + \ldots + s_i$$

pour tout entier $i \geq 1$. Nous aurons également besoin des *nombres de Kotska* $K_{\lambda s}$ qui sont le nombre de tableaux généralisés semi-standards de type λ et de composition s :

$$K_{\lambda s} = |T'_{\lambda s}|$$

Théorème 6

$$\mathbb{C}[X_s] \simeq \bigoplus_{\lambda \trianglerighteq s} K_{\lambda s}[\lambda].$$

Pour éviter toute confusion, nous noterons V_λ^s le sous-espace de $\mathbb{C}[X_s]$ isomorphe à $K_{\lambda s}[\lambda]$:

$$\mathbb{C}[X_s] = \bigoplus_{\lambda \trianglerighteq s} V_\lambda^s$$

Cas binaire. Considérons le cas où $q = 2$; les mots n'ont que des 1 et des 2, les partitions ont au plus deux termes et les tabloïdes n'ont que deux lignes. Nous appellerons ce cas le *cas binaire*. Dans cette situation il n'y a, pour tout type et toute composition, qu'un éventuel tableau semi-standard ; il est de la forme :

$$t = \begin{array}{cc} 111 & \ldots 1 \quad 222 \ldots 2 \\ \underbrace{222}_{k} & \end{array}$$

Ainsi dans ce cas particulier toutes les multiplicités sont égales à un :

$$\mathbb{C}[X_{(n-w,w)}] \simeq \bigoplus_{k \leq w} [n-k, k]$$

(avec $w \leq n/2$ pour garantir que $(n-w, w)$ est bien une partition).
Ce fait est important, nous y reviendrons par la suite (cf. 3.5).

Description de V_λ^s

Le module de Specht $[\lambda]$ est par définition (cf. 1.3) un sous-espace de $\mathbb{C}[\mathcal{T}_\lambda]$ ou, si l'on veut, de $\mathbb{C}[X_\lambda]$. Mais il est possible de l'envoyer dans $\mathbb{C}[\mathcal{T}_s]$ grâce à un opérateur explicite.
Soit t_λ le tableau dont la $i^{ième}$ ligne est formée des entiers $\lambda_1 + \ldots + \lambda_{i-1} + 1, \ldots, \lambda_1 + \ldots + \lambda_{i-1} + \lambda_i$.

Exemple : $s = (3,2,1), t_s = \begin{array}{l}123\\45\\6\end{array}$.

Ainsi le tabloïde $\overline{t_\lambda}$ correspond au mot x_λ défini en 1.4 via la bijection vue en 1.2. Il est clair que tout tabloïde de type λ peut être obtenu à partir de t_λ par application d'une permutation convenablement choisie : on dit que $\mathcal{T}_\lambda$ est *cyclique*. On définit alors, à partir de chaque tableau généralisé $t \in T_{\lambda s}$, un S_n-homomorphisme $\theta_t : \mathbb{C}[\mathcal{T}_\lambda] \to \mathbb{C}[T_{\lambda s}]$ en posant : $\theta_t(\overline{t_\lambda}) = \sum_{t' \sim t} t'$. La relation $\sim$ a été définie en 1.2 ; l'extension de θ_t à tout $\mathbb{C}[\mathcal{T}_\lambda]$ se fait par cyclicité puis linéarité. A priori θ_t arrive dans $\mathbb{C}[T_{\lambda s}]$, mais on a vu en 1.2 qu'il existait une bijection très simple entre cet espace et $\mathbb{C}[X_s]$ ou même $\mathbb{C}[\mathcal{T}_s]$. C'est pourquoi nous considérerons dans la suite que θ_t arrive directement dans n'importe lequel de ces trois espaces.

Théorème 7 *L'ensemble des applications $\{\theta_t, t \in T'_{\lambda s}\}$ est une base de l'espace des S_n-homomorphismes de $[\lambda]$ dans $\mathbb{C}[X_\lambda]$:*

$$\bigoplus_{t \in T'_{\lambda s}} \theta_t([\lambda]) = V_\lambda^s$$

Cas binaire : introduisons la relation d'ordre suivante sur les mots binaires : nous dirons que $y \succeq x$ pour $x, y \in \mathcal{F}_2^n$ si $x_i = 1$ ou y_i pour tout i dans $1, \ldots, n$. Définissons également le *poids* d'un mot comme le nombre de 2 qu'il contient ; c'est en fait l'équivalent de la composition dans le cas binaire. Aussi désignons-nous, pour tout entier k, l'ensemble des mots de poids k par X_k. Considérons enfin, pour tout entier $w \geq k$, l'opérateur ψ_w défini sur X_k par :

$$\psi_w(x) = \sum_{y \in X_w, y \succeq x} y.$$

Cet opérateur est utilisé notamment dans [1] et [8]. Dans le cas binaire, l'opérateur θ_t défini à partir de l'unique tableau semi-standard :

$$t = \begin{array}{l}111 \quad \ldots 1 \quad 222 \ldots 2\\ \underbrace{222}_{k}\end{array}$$

vu dans la section précédente correspond à ψ_k. En effet les tableaux $t' \sim t$ s'obtiennent à partir de t en permutant simplement les termes de sa première ligne ; d'où, en confondant mots et tableaux généralisés : $\theta_t(\overline{t_{(n-k,k)}}) = \psi_w(x_{(n-k,k)})$ où w désigne le nombre total de 2 dans t. Finalement, par cyclicité : $\theta_t = \psi_w$.
Nous verrons dans la deuxième partie (paragraphe 4.5) d'autres opérateurs permettant de relier V_λ^s à $[\lambda]$.

Chapitre 2

Fonctions harmoniques

2.1 Fonctions zonales, fonctions sphériques

Soit $L(X_s)$ l' espace vectoriel des fonctions à valeurs complexes définies sur X_s :

$$L(X_s) = \{f : X_s \to \mathbb{C}\}.$$

Le groupe symétrique $G = S_n$ agit à gauche sur $L(X_s)$:

$$(\sigma.f)(x) = f(\sigma^{-1}x) \quad \forall \sigma \in S_n, \forall f \in L(X_s)$$

et nous avons bien sûr les S_n-isomorphismes :

$$L(X_s) \simeq \mathbb{C}[X_s] \simeq \bigoplus_{\lambda \trianglerighteq s} K_{\lambda s}[\lambda].$$

Le premier isomorphisme est très simple ; il est donné par : $f \mapsto \sum_{x \in X_s} f(x)x$. Mais, pour éviter tout risque de confusion nous noterons W_λ^s le sous-espace de $L(X_s)$ isomorphe à $K_{\lambda s}[\lambda]$. En revanche, pour alléger les notations nous considérerons que l'opérateur θ_t défini en 1.4 arrive directement dans $L(X_s)$. Soit $H = S_s \simeq S_{s_1} \times \ldots \times S_{s_q}$ le stabilisateur dans S_n du mot x_s défini en 1.4. Une fonction f de $L(X_s)$ est dite *zonale* si : $h.f = f$ pour tout h dans H.
Une fonction zonale est dite *sphérique* si elle est élément de l'un des sous-espaces W_λ^s.
Une fonction à la fois zonale et sphérique est dite *harmonique*. Nous noterons $[W_\lambda^s]^H$ l'espace des fonctions harmoniques. La proposition suivante, qui donne la dimension de cet espace, est une conséquence immédiate de la formule de Frobenius.

Proposition *La dimension de l'espace des fonctions harmoniques est :*

$$dim[W_\lambda^s]^H = K_{\lambda s}^2$$

Ainsi y-a-t-il, dans le cas binaire, une unique fonction zonale par composante. Cette fonction coïncide en fait avec certains polynômes appelés *polynômes de Hahn* (cf. deuxième partie, paragraphe 4.3).
La proposition précédente montre également qu'une base de fonctions harmoniques contient autant d'éléments que l'ensemble des couples de tableaux semi-standards $T_{\lambda s}$. Nous donnerons dans ce chapitre (paragraphe 2.3) une bijection explicite entre ces deux ensembles.
Le groupe S_s est le stabilisateur de l'élément x_s ; nous avons défini cet élément pour simplifier l'exposé mais en fait nous aurions tout aussi bien pu considérer S_s comme le stabilisateur d'un quelconque élément $x_0 \in X_s$. Cela étant dit, la notion de fonction zonale dépend du groupe S_s donc du choix de cet élément. On peut éviter cela en travaillant non plus sur X_s mais sur $X_s \times X_s$: une fonction $F \in L(X_s \times X_s)$ sera dite zonale si :

$$F(gx, gy) = F(x, y) \quad \forall g \in G \quad \forall x, y \in X_s.$$

Il est clair que si F est zonale alors pour tout $x_0 \in X_s$ la fonction $y \mapsto F(x_0, y)$ est aussi zonale. Réciproquement, étant donnée une fonction zonale f relativement au stabilisateur d'un élément x_0, on obtient une fonction zonale $(x, y) \mapsto F(x, y)$ en posant :

$$\begin{cases} F(x_0, y) = f(y) & \forall y \in X_s \\ F(gx, gy) = F(x, y) & \forall g \in G \quad \forall x, y \in X_s \end{cases}$$

Ainsi une fonction zonale F est-elle invariante par la transformation $(x, y) \mapsto (gx, gy)$. Aussi ne dépend-elle pas véritablement du couple (x, y) mais plutôt de l'orbite de celui-ci sous l'action de G ; d'où l'intérêt de remplacer le couple (x, y) par un représentant plus commode :

Définition 12 *Pour tout x, y dans $\mathcal{F}_q^n$ on note $N(x, y)$ la matrice de taille $q \times q$ dont le coefficient situé sur la $i^{ième}$ ligne et la $j^{ième}$ colonne est $|\{k, x_k = i, y_k = j\}|$.*

Théorème 8 *Soient x, y, x', y' des éléments de $\mathcal{F}_q^n$*

$$\exists \sigma \in G \quad x' = \sigma x, y' = \sigma y \Leftrightarrow N(x, y) = N(x', y')$$

Preuve :
($\Rightarrow$) : nous avons pour tout i, j :

$$N_{i,j}(\sigma x, \sigma y) = |\{k, (\sigma x)_k = i, (\sigma y)_k = j\}| = |\{l, x_l = i, y_l = j\}| = N_{i,j}(x, y)$$

($\Leftarrow$) : soit $\mathcal{C}_{i,j}(x,y)$ l'ensemble de coordonnées défini par :

$$\mathcal{C}_{i,j}(x,y) = \{k, x_k = i, y_k = j\}$$

ainsi $N_{i,j}(x,y) = |\mathcal{C}_{i,j}(x,y)|$; pour tout i,j nous avons $|\mathcal{C}_{i,j}(x',y')| = |\mathcal{C}_{i,j}(x,y)|$ et les ensembles $\mathcal{C}_{i,j}(x,y)$ forment une partition de $\{1,\ldots,n\}$ donc il est possible de trouver un $\sigma \in G$ tel que $\sigma\mathcal{C}_{i,j}(x',y') = \mathcal{C}_{i,j}(x,y)$ pour tout i,j. Avec un tel σ, nous avons : $x' = \sigma x, y' = \sigma y$. □

Ainsi les fonctions harmoniques ne dépendent-elles que de $N(x_s,y)$; il s'avère qu'elles sont en fait des fonctions polynomiales des coefficients de $N(x_s,y)$ (cf. théorème 10).

2.2 Une base de vecteurs harmoniques

Considérons l'application $\psi : T_\lambda \to T_{\lambda s}$ qui remplace les coefficients *"i"* d'un tableau généralisé par la $i^{ième}$ coordonnées du mot x_s.
Exemple :

$$s = (4,3,2), x^s = (1,1,1,1,2,2,2,3,3), \lambda = (5,2,2)$$

$$t = \begin{array}{l} 12568 \\ 34 \\ 79 \end{array} \qquad \psi(t) = \begin{array}{l} 11223 \\ 11 \\ 23 \end{array}$$

Cet exemple montre que l'image d'un tableau *standard* n'est pas nécessairement un tableau *semi-standard*. De la définition même de ψ il suit :

$$\psi(\sigma t) = \psi(t) \quad \forall \sigma \in S_s$$

l'action de S_s se faisant sur les *coefficients* du tableau t. Par ailleurs il est aisé de voir que ψ est surjective et qu'un tableau généralisé semi-standard admet toujours dans ses antécédents un tableau standard. Pour simplifier nous noterons $\{T_i, 1 \le i \le K_{\lambda s}\}$ l'ensemble des tableaux semi-standards et $\{t_i, 1 \le i \le K_{\lambda s}\}$ un ensemble de tableaux standards tels que $\psi(t_i) = T_i$ pour tout i. L'application ψ induit une application

$$\begin{array}{rccc} \widetilde{\psi}: & \mathcal{T}_\lambda & \longrightarrow & \mathcal{T}_{\lambda s} \\ & \overline{T} & \mapsto & \widetilde{\psi}\,(\overline{T}) = \overline{\psi(T)} \end{array}$$

que l'on étend à $\mathbb{C}[\mathcal{T}_\lambda]$ par linéarité. Soit ε_H l'opérateur $\frac{1}{|H|}\sum_{\sigma\in H}\sigma$; on pose :

$$u_{i,j} = \theta_{T_j}(\varepsilon_H e_{t_i}).$$

Théorème 9 *La famille de vecteurs $(u_{i,j})_{i,j}$ est une base de $(V_\lambda^s)^H$.*

Plan de la preuve : il suffit de montrer que la famille est libre ; nous la remplaçons grâce à l'application $\widetilde{\psi}$ par une famille plus simple à étudier ; nous concluons par l'absurde, en munissant $\mathcal{T}_{\lambda s}$ d'un ordre total à l'aide d'un lemme permettant de comparer des tabloïdes généralisés issus de T_i et son antécédent t_i.

Preuve :
par construction $u_{i,j} \in (V_\lambda^s)^H$. En outre :

$$V_\lambda^s = \bigoplus_j \theta_{T_j}(V_\lambda^\lambda)$$

il suffit donc de prouver que les $\varepsilon_H e_{t_i}$ forment une famille libre puisque $|\{u_{i,j}\}| = K_{\lambda s}^2$. Comme ψ est H-invariant, $\widetilde{\psi}$ est aussi H-invariant et donc :

$$\widetilde{\psi}\left(\varepsilon_H e_{t_i}\right) = \widetilde{\psi}\left(e_{t_i}\right)$$

Rappelons que :

$$e_{t_i} = \sum_{\tau \in C(t_i)} \varepsilon(\tau)\overline{\tau.t_i}$$

donc

$$\begin{aligned}\widetilde{\psi}\left(e_{t_i}\right) &= \sum_{\tau \in C(t_i)} \varepsilon(\tau)\ \widetilde{\psi}\left(\overline{\tau.t_i}\right) \\ &= \sum_{\tau \in C(t_i)} \varepsilon(\tau)\overline{\psi(\tau.t_i)}\end{aligned}$$

Nous munissons alors $\mathcal{T}_{\lambda s}$ d'un ordre total de la façon suivante : à $\overline{T} \in \mathcal{T}_{\lambda s}$ nous associons un élément de $T_{\lambda s}$ en ordonnant les lignes de $\overline{T}$.
Exemple :

$$\overline{T} = \begin{array}{ll} \overline{212} & \\ \overline{32} & \mapsto \\ \overline{12} & \end{array} \begin{array}{l} 122 \\ 23 \\ 12 \end{array}$$

Nous introduisons alors un ordre total sur $\mathcal{T}_{\lambda s}$ de la façon suivante : nous dirons que $\overline{T} \geq \overline{T'}$ si, après avoir ordonné les lignes de T et T', la première ligne (en partant du haut) qui n'est pas la même dans T et T' est plus grande - au sens de l'ordre lexicographique - dans T.
Exemple :

$$\begin{array}{ll} \overline{212} & \\ \overline{32} & > \\ \overline{12} & \end{array} \begin{array}{l} \overline{122} \\ \overline{31} \\ \overline{22} \end{array}$$

car $23 > 13$ au sens de l'ordre lexicographique.
Lemme *Pour T_i dans $T'_{\lambda s}$ et t_i son antécédent nous avons :*

$$\overline{\psi(\tau.t_i)} > \overline{T_i} \quad \forall \tau \in C(t_i),\ \tau \neq id$$

Preuve :
les colonnes de T_i croissent strictement et les coefficients de la première ligne L de $\psi(\tau.t_i)$ différente de la ligne correspondante de T_i sont nécessairement l'image par τ de coefficients situés *en-dessous* de L. Donc, une fois que L a été ordonnée dans $\psi(\tau.t_i)$, elle est forcément supérieure - au sens de l'ordre lexicographique - à son analogue dans T_i. □

Si $\tau \neq$ id, $\psi(\tau.t_i) \neq T_i$ car les colonnes de T_i croissent strictement. Donc $\overline{T_i}$ apparaît dans $\widetilde{\psi}\ (e_{t_i})$ avec un coefficient non-nul.
Supposons àprésent qu'il existe des λ_i non tous nuls tels que :

$$\sum_i \lambda_i\ \widetilde{\psi}\ (e_{t_i}) = 0.$$

Soit $\overline{T_0} = \overline{\psi(t_0)}$ le plus petit élément de $\{\overline{\psi(t_i)} | \lambda_i \neq 0\}_i$. Ainsi $\overline{T_i} > \overline{T_0}$ si $t_i \neq t_0$ ce qui implique $\overline{\psi(\tau t_i)} > \overline{T_0}$ si $t_i \neq t_0$; en outre $\overline{\psi(\tau.t_0)} > \overline{T_0}$ pour tout τ dans $C(t_i)$, $\tau \neq$ id.
Donc $\overline{T_0}$ apparaît avec un coefficient $\lambda_0 \neq 0$ dans :

$$\sum_i \lambda_i\ \widetilde{\psi}\ (e_{t_i}) = \sum_i \sum_{\tau \in C(t_i)} \lambda_i \varepsilon(\tau) \overline{\psi(\tau.t_i)}$$

et cette somme n'est pas nulle, contradiction. □

2.3 Formules explicites

Dans ce qui suit nous ne tiendrons pas compte de la première ligne des tableaux généralisés que nous considérerons ; par conséquent nous notons :

$$t = \begin{array}{l} \times \times \cdots \times \times \\ a_1 a_2 \cdots a_{\lambda_2} \\ \cdots\cdots \\ \cdots\ a_{n-\lambda_1} \end{array} \qquad t' = \begin{array}{l} \times \times \cdots \times \times \\ b_1 b_2 \ldots b_{\lambda_2} \\ \cdots\cdots \\ \cdots\ b_{n-\lambda_1} \end{array}$$

deux tableaux généralisés de type λ et de composition s. Dans le cas où t et t' sont semi-standards - cas qui nous intéresse - nous ne perdons pas

d'information puisque la première ligne peut être déduite des autres.
introduisons à présent quelques notations :

- $c_{k,l} = |\{i, a_i = k, b_i = l\}|$ avec $1 \leq k, l \leq q$ (si t et t' sont semi-standards alors $c_{1,l} = c_{k,1} = 0$).
- $c_k = \sum_{l=1}^{q} c_{k,l} = |\{i, a_i = k\}|$ pour $1 \leq k \leq q$.
- $(a)_k$ est la notation habituelle pour : $a(a-1)\dots(a-k+1)$.

Définition 13 *Nous notons $A_{t,t'}$ la fonction définie sur les matrices $N = (N[k,l])_{k,l}$ de taille $q \times q$ à coefficients entiers par :*

$$A_{t,t'}(N) = \prod_{k=1}^{q} \frac{\prod_{l=1}^{q} (N[k,l])_{c_{k,l}}}{(s_k)_{c_k}}$$

Posons à présent :

$$S'_\lambda = S_{\lambda_2} \times \cdots \times S_{\lambda_l}$$

$$S_{\lambda^*} = S_{\lambda^*_1} \times \cdots \times S_{\lambda^*_{\lambda_1}}$$

où λ^* est la partition déduite de λ en transposant son diagramme (cf. 1.2). S'_λ agit sur les tableaux généralisés par permutation des lignes (la première restant inchangée) tandis que S_{λ^*} agit par permutation des colonnes.

Définition 14 *Nous notons $F_{t,t'}$ la fonction définie sur les matrices de taille $q \times q$ à coefficients entiers par :*

$$F_{t,t'} = \sum_{\substack{\sigma \in S_{\lambda^*} \\ \tau \in S'_\lambda}} \varepsilon(\sigma) A_{\sigma t, \tau t'}.$$

Relions à présent les fonctions $F_{t,t'}$ aux vecteurs $u_{i,j}$ vus au paragraphe précédent.

Théorème 10 *Nous avons :*

$$u_{i,j} = \sum_{y \in X_s} F_{T_i,T_j}(x_s, y) y$$

autrement dit la famille de fonctions $\{F_{t,t'}, (t,t') \in (T^s_{\lambda s})^2\}$ est une base de fonctions harmoniques.

2.4 Preuve du théorème 10

Il s'agit en fait de compter combien de fois un mot y apparaît dans les vecteurs harmoniques $u_{i,j} = \theta_{T_j}(\varepsilon_H e_{t_i})$ du théorème 9. Commençons par un exemple concret :

$$\lambda = (3,2,1),\ s = (2,2,2),\quad T_j = \begin{array}{l}112\\23\\3\end{array} \in T_{\lambda s},\ t_i = \begin{array}{l}124\\35\\6\end{array} \in T_\lambda$$

$$\theta_{T_j}\begin{array}{l}\overline{123}\\\overline{45}\\\overline{6}\end{array} \overset{déf}{=} \begin{array}{l}112\\23\\3\end{array} + \begin{array}{l}121\\23\\3\end{array} + \begin{array}{l}211\\23\\3\end{array} + \begin{array}{l}112\\32\\3\end{array} + \begin{array}{l}121\\32\\3\end{array} + \begin{array}{l}211\\32\\3\end{array}$$

$$\overline{t_i} = (3,4)\ \begin{array}{l}\overline{123}\\\overline{45}\\\overline{6}\end{array} \Rightarrow \theta_{T_j}\overline{t_i} = \begin{array}{l}112\\23\\3\end{array} + \begin{array}{l}122\\13\\3\end{array} + \begin{array}{l}212\\13\\3\end{array} + \begin{array}{l}113\\22\\3\end{array} + \begin{array}{l}123\\12\\3\end{array} + \begin{array}{l}213\\12\\3\end{array}$$

Rappelons que l'on peut identifier $T_{\lambda s}$ et X_s quelque soit λ (cf. 1.2). Ainsi, $\theta_{T_j}\begin{array}{l}\overline{123}\\\overline{45}\\\overline{6}\end{array}$ est la somme de :

- tous les mots de X_s dont les trois derniers termes sont 2,3,3
- tous les mots de X_s dont les trois derniers termes sont 3,2,3

et $\theta_{T_j}\overline{t_i}$ est la somme de :

- tous les mots de X_s dont le $3^{ième}$ terme est 2, le $5^{ième}$ est 3 et le $6^{ième}$ est 3
- tous les mots de X_s dont le $3^{ième}$ terme est 3, le $5^{ième}$ est 2 et le $6^{ième}$ est 3.

Dans le cas général, si l'on note :

$$t_i = \begin{array}{l}\times\times\cdots\times\times\\a_1a_2\cdots a_{\lambda_2}\\\cdots\cdots\\\cdots\ a_{n-\lambda_1}\end{array} \qquad T_j = \begin{array}{l}\times\times\cdots\times\times\\b_1b_2\ldots b_{\lambda_2}\\\cdots\cdots\\\cdots\ b_{n-\lambda_1}\end{array}$$

on voit que $\theta_{T_j}(\overline{t_i})$ est la somme de :

- tous les mots de X_s dont le $a_1^{ième}$ terme est b_1, le $a_2^{ième}$ est b_2,..., le $a_{n-\lambda_1}^{ième}$ est $b_{n-\lambda_1}$,
- d'autres termes que l'on peut déduire en permutant les coefficients dans les lignes de t_i.

Soit $\theta^1_{T_j}(t_i)$ le premier terme de cette somme : $\theta^1_{T_j}(t_i)$ est donc la somme de tous les mots de X_s dont le $a_1^{ième}$ terme est b_1, le $a_2^{ième}$ est b_2,..., le $a_{n-\lambda_1}^{ième}$ est

$b_{n-\lambda_1}$.
Nous avons raisonné sur t_i et $T_j = \psi(t_j)$ mais il est clair que ce qui précède est vrai en fait si l'on remplace t_i par n'importe quel tableau de type λ et T_j par n'importe quel tableau généralisé de type λ et de composition s.
Introduisons quelques notations :

- $\mathcal{C}_{k,l}$ est l'ensemble des a_m (pour $m \in \{1, \ldots, n-\lambda_1\}$) tels que le $a_m^{ième}$ terme de x_s est k et tels que $b_m = l$
- $c_{k,l} = |\mathcal{C}_{k,l}|$ est le nombre de k dans T_i correspondant à un l dans T_j,
- $c_k = \sum_l c_{k,l}$: c'est le nombre de "k" dans T_i qui ne sont pas dans sa première ligne,

et pour un mot y :

- $\mathcal{C}_{k,l}(y)$ est l'ensemble des coordonnées $m \in \{1, \ldots, n-\lambda_1\}$ telles que le $m^{ième}$ terme de x_s soit k et le $m^{ième}$ terme de y soit l ; donc $|\mathcal{C}_{k,l}(y)| = N[k,l]$ où $N[k,l]$ est le $(k,l)^{ième}$ coefficient de $N(x_s, y)$.

Maintenant calculons combien de fois un mot donné y apparaît dans $\varepsilon_H \theta^1_{T_j}(t_i)$.
On a :

$$\theta^1_{T_j}(t_i) = \sum_{y \in A} y$$

où A est l'ensemble : $A = \{y, \mathcal{C}_{k,l}(y) \supset \mathcal{C}_{k,l} \ \forall k, l\}$.
Soit $\sigma \in H$:

$$\sigma\theta^1_{T_j}(t_i) = \sum_{y \in A} \sigma y$$

$$= \sum_{y \in B} y$$

avec :

$$B \overset{déf}{=} \{y, \mathcal{C}_{k,l}(\sigma^{-1}y) \supset \mathcal{C}_{k,l} \ \forall k, l\}$$

$$= \{y, \sigma\mathcal{C}_{k,l}(y) \supset \mathcal{C}_{k,l} \ \forall k, l\}$$

$$= \{y, \mathcal{C}_{k,l}(y) \supset \sigma^{-1}\mathcal{C}_{k,l} \ \forall k, l\}$$

Un mot y apparaît dans cette somme si et seulement si $\mathcal{C}_{k,l}(y) \supset \sigma^{-1}\mathcal{C}_{k,l}$ pour tout k, l. En outre l'on somme sur y donc un mot y napparaît qu'une fois au plus. Donc :

$$\varepsilon_H \theta^1_{T_j}(t_i) = \frac{1}{|H|} \sum_y \sum_{\sigma, \sigma\mathcal{C}_{k,l} \subset \mathcal{C}_{k,l}(y) \forall k,l} y$$

Pour qu'un mot y apparaisse il faut :

- choisir un sous-ensemble $\{\mathcal{C}'_{k,l}\}_{k,l}$ tel que $\mathcal{C}'_{k,l} \subset \mathcal{C}_{k,l}(y)$ (ce qui correspond à $\sigma\mathcal{C}_{k,l} \subset \mathcal{C}_{k,l}(y) \forall k, l$) : $\prod_{k,l} \binom{N[k,l]}{c_{k,l}}$ possibilités ;

– choisir une permutation σ qui envoie pour tout k, l l'ensemble $\mathcal{C}_{k,l}$ sur l'ensemble $\{\mathcal{C}'_{k,l}\}_{k,l}$ défini au-dessus : $\prod_k \prod_l c_{k,l}!(s_k - \sum_l c_{k,l})!$ possibilités.

Le résultat de ce calcul est :

$$\frac{1}{|H|} \prod_{k,l} c_{k,l}! \binom{N[k,l]}{c_{k,l}} (s_k - \sum_l c_{k,l})!$$

$$= \prod_k \frac{(s_k - \sum_l c_{k,l})!}{s_k!} \prod_l \frac{N[k,l]!}{(N[k,l] - c_{k,l})!}$$

$$= \prod_{k=1}^{q} \frac{\prod_{l=1}^{q} (N[k,l])_{c_{k,l}}}{(s_k)_{c_k}}$$

Ce polynôme en les coefficients de $N(x_s, y)$ défini à partir de t_i et T_j ne dépend en fait que de $T_i = \psi(t_i)$ et T_j. C'est en fait le polynôme A_{T_i,T_j} défini en 10. Il correspond donc à $\varepsilon_H \theta^1_{T_j}(t_i)$; pour obtenir les autres termes de $\theta_{T_j}(\overline{t_i})$ nous n'avons qu'à remplacer $\overline{t_i}$ par e_{t_i} (dont le premier terme est précisément $\overline{t_i}$). Nous obtenons finalement le polynôme :

$$\sum_{\substack{\sigma \in S_{\lambda^*} \\ \tau \in S'_\lambda}} \varepsilon(\sigma) A_{\sigma T_i, \tau T_j}$$

qui est bien $F_{T_i,T_j}(x_s, y)$. □

2.5 Cas particuliers

Cas binaire

Calculons dans le cas binaire la fonction harmonique F_k du module $W_{(n-k,k),(n-w,w)}$ dans la décomposition :

$$L(X_{(n-w,w)}) = \bigoplus_{k \leq w} W^{(n-w,w)}_{(n-k,k)} \simeq \bigoplus_{k \leq w} [n-k, k].$$

Soient T et u deux mots de poids w, nous avons :

$$N(T,u) = \begin{pmatrix} n - 2w + |T \cap u| & w - |T \cap u| \\ w - |T \cap u| & |T \cap u| \end{pmatrix}$$

Posons $t = \underbrace{111\ldots1\ 222\ldots2}_{k}$

on a :

$$F_k(T,u) = F_{t,t}(T,u) = \sum_{i=0}^{k} (-1)^i \frac{\binom{|T\cap u|}{k-i}\binom{w-|T\cap u|}{i}}{\binom{w}{k-i}\binom{n-w}{i}} \binom{k}{i}$$

En fait F_k correspond aux polynômes de Hahn définis par :

$$Q_k(i) = m_k \sum_{j=0}^{k} (-1)^j \frac{\binom{k}{j}\binom{n+1-k}{j}}{\binom{w}{j}\binom{n-w}{j}} \binom{i}{j}$$

avec $m_k = \binom{n}{k} - \binom{n}{k-1}$. En effet P. Delsarte a montré dans [8] que ces polynômes étaient les fonctions harmoniques de cette représentation (cf. 4.3). Plus précisément on a :

$$m_k F_{t,t}(N(x,y)) = Q_k(w - |x \cap y|).$$

Cas des modules $[k,\ldots,k]$

Considérons à présent les modules $[\lambda]$ où $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_l)$ est une partition telle que $l = q$ et $\lambda_2 = \ldots = \lambda_l = k$, k étant un entier inférieur à λ_1 :

$$\lambda = (\lambda_1, \underbrace{k,\ldots,k}_{q-1}).$$

Il est aisé de voir que la multiplicité $K_{\lambda,s}$ d'un tel module est au plus un pour tout $s = (s_1,\ldots,s_q)$: en effet le seul éventuel tableau semi-standard de type λ ayant ses coefficients dans $\{1,\ldots,q\}$ est :

$$T_k = \begin{array}{l} 111 * ** \\ 222 \\ \vdots \\ \underbrace{qqq}_{k} \end{array}$$

considérons alors l'opérateur ψ défini par :

$$\psi(X^l) = (X)_l = X(X-1)\ldots(X-l+1)$$

pour n'importe quelle indéterminée (formelle) X dans $\{N[i,j], s_i \,|\, i,j\ in\ 1,\ldots,q\}$ et étendu à la base de $\mathbb{C}[N[i,j], s_i \,|\, i,j\ in\ 1,\ldots,q]$ via :

$$\psi(\prod_{i,j} N[i,j]^{c_{i,j}} s_i^{c_i}) = \prod_{i,j} \psi(N[i,j]^{c_{i,j}}) \psi(s_i^{c_i})$$

et enfin étendu à $\mathbb{C}[N[i,j], s_i \,|\, i,j \; in \; 1,\ldots,q]$ par linéarité :
Nous avons donc :

$$F_{T_k,T_k}(N) = \sum_{\sigma_1,\ldots,\sigma_k \in S_q} \varepsilon(\sigma_1)\ldots\varepsilon(\sigma_k) \frac{\prod_{j=2}^{q} \psi(N[\sigma_1(j),j]\ldots N[\sigma_k(j),j])}{\psi(\prod_{i=2}^{q} s_{\sigma_1(i)} s_{\sigma_2(i)} \ldots s_{\sigma_k(i)})}$$

qui apparaît à présent comme un polynôme en les $N[i,j]$ et une fonction rationnelle en les s_i. Cependant, dans la définition 13 la composition est fixée, aussi les dénominateurs $(s_i)_{c_i}$ sont-ils des constantes scalaires et il est possible de les faire disparaître car les fonctions harmoniques sont définies à multiplication par un scalaire près :

Définition 15 *On note f_k la fonction harmonique $\psi(\prod_{i=1}^{q} s_i^k) \times F_{T_k,T_k}$.*

Comme nous le verrons dans le prochain théorème (cf. 11), cette fonction peut être reliée au *déterminant*.
Soit $Q \in \mathbb{C}[x_1,\ldots,x_r]$ un polynôme à r indéterminées, on peut lui associer un opérateur différentiel $Q(\partial)$: il suffit d'envoyer chaque monôme $x_1^{i_1}\ldots x_r^{i_r}$ sur $\frac{\partial^{i_1+\ldots+i_r}}{\partial x_1^{i_1}\ldots\partial x_r^{i_r}}$ (on envoie la constante 1 sur *identité*).
Soit Res l'opérateur de *restriction* de $\mathbb{C}[X_{i,j}, (i,j) \in \mathcal{F}_q \times \mathcal{F}_q]$ dans $\mathbb{C}[X_i, i \in \mathcal{F}_q]$ défini par $X_{i,j} \mapsto X_i$ pour tout j dans $\mathcal{F}_q$.

Théorème 11 *Soient $u, v \in X_s$ et soit N la matrice $N(u,v)$ dont on note $N[i,j]$ le terme général. On a :*

$$\text{Res } \text{Det}^k(\partial) \prod_{i,j=1}^{q} X_{i,j}^{N[i,j]} = f_k(N) \prod_i X_i^{s_i-k}$$

Preuve :
si l'on considère :

$$\frac{\psi(\prod_{i=1}^{q} s_i^k)}{\psi(\prod_{i=2}^{q} s_{\sigma_1(i)} s_{\sigma_2(i)} \ldots s_{\sigma_k(i)})}$$

il est facile de voir que les seuls termes que le dénominateur ne contient pas sont : $s_{\sigma_1(1)} s_{\sigma_2(1)} \ldots s_{\sigma_k(1)}$; par conséquent soit $r_i = |\{l = 1,\ldots,k \,|\, \sigma_l(1) = i\}|$ on a alors :

$$\frac{\psi(\prod_{i=1}^{q} s_i^k)}{\psi(\prod_{i=2}^{q} s_{\sigma_1(i)} s_{\sigma_2(i)} \ldots s_{\sigma_k(i)})} = \prod_{r_i \neq 0} (s_i - k + r_i)\ldots(s_i - k + 1).$$

On calcule alors Res $\text{Det}^k(\partial) \prod_{i,j} X_{i,j}^{N[i,j]}$ et l'on montre que l'on obtient $f_k(N) \prod_i X_i^{s_i-k}$:

$$\text{Det}^k \begin{pmatrix} \frac{\partial}{\partial X_{1,1}} & \frac{\partial}{\partial X_{1,2}} & \cdots \\ \frac{\partial}{\partial X_{2,1}} & \frac{\partial}{\partial X_{2,2}} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \prod_{i,j} X_{i,j}^{N[i,j]}$$

$$= \mathrm{Det}^k \begin{pmatrix} \frac{\partial}{\partial X_{1,1}} + \frac{\partial}{\partial X_{1,2}} + \ldots + \frac{\partial}{\partial X_{1,q}} & \frac{\partial}{\partial X_{1,2}} & \cdots \\ \frac{\partial}{\partial X_{2,1}} + \frac{\partial}{\partial X_{2,2}} \ldots + \frac{\partial}{\partial X_{2,q}} & \frac{\partial}{\partial X_{2,2}} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \prod_{i,j} X_{i,j}^{N[i,j]}$$

$$= [\sum_{\sigma \in S_q} \varepsilon(\sigma)(\frac{\partial}{\partial X_{\sigma(1),1}} + \ldots + \frac{\partial}{\partial X_{\sigma(1),q}}) \prod_{j=2}^{q} \frac{\partial}{\partial X_{\sigma(j),j}}]^k \prod_{i,j} X_{i,j}^{N[i,j]}$$

$$= \sum_{\sigma_1,\ldots,\sigma_k \in S_q} \varepsilon(\sigma_1)\ldots\varepsilon(\sigma_k)(\frac{\partial}{\partial X_{\sigma_1(1),1}} + \ldots + \frac{\partial}{\partial X_{\sigma_1(1),q}}) \ldots (\frac{\partial}{\partial X_{\sigma_k(1),1}} + \ldots + \frac{\partial}{\partial X_{\sigma_k(1),q}})$$

$$\times \textstyle\prod_{j=2}^{q} \frac{\partial}{\partial X_{\sigma_1(j),j}} \cdots \frac{\partial}{\partial X_{\sigma_k(j),j}} \prod_{i,j} X_{i,j}^{N[i,j]}$$

Donc, si l'on applique l'opérateur ψ aux $N[i,j]$ considérés comme indéterminées nous obtenons alors pour $\prod_{j=2}^{q} \frac{\partial}{\partial X_{\sigma_1(j),j}} \cdots \frac{\partial}{\partial X_{\sigma_k(j),j}} \prod_{i,j} X_{i,j}^{N[i,j]}$:

$$\prod_{j=2}^{q} \psi(N[\sigma_1(j),j] \ldots N[\sigma_k(j),j]) \prod_{i=1}^{q} (X_{i,1}^{N[i,1]} \prod_{j=2}^{q} X_{i,j}^{N[i,j]-|\{l,\sigma_l(j)=i\}|})$$

Il faut à présent appliquer aux indéterminées l'opérateur :

$$(\frac{\partial}{\partial X_{\sigma_1(1),1}} + \ldots + \frac{\partial}{\partial X_{\sigma_1(1),q}}) \ldots (\frac{\partial}{\partial X_{\sigma_k(1),1}} + \ldots + \frac{\partial}{\partial X_{\sigma_k(1),q}}) = \prod_{r_i \neq 0} (\frac{\partial}{\partial X_{i,1}} + \ldots + \frac{\partial}{\partial X_{i,q}})^{r_i}.$$

Avec l'aide de :

$$\sum_j N[i,j] = s_i \qquad r_i + \sum_{j \geq 2} |\{l, \sigma_l(j) = i\}| = k$$

vrai pour tout i on trouve :

$$\prod_{r_i \neq 0} (s_i - k + r_i) \ldots (s_i - k + 1) \prod_{i=1}^{q} (X_{i,1}^{N[i,1]-r_i} \prod_{j=2}^{q} X_{i,j}^{N[i,j]-|\{l,\sigma_l(j)=i\}|-r_i})$$

et en utilisant $\sum_i r_i = k$ après restriction on conclut :

Res $\mathrm{Det}^k(\partial) \prod_{i,j} X_{i,j}^{N[i,j]} =$

$$\sum_{\sigma_1,\ldots,\sigma_k \in S_q} \varepsilon(\sigma_1)\ldots\varepsilon(\sigma_k) \prod_{r_i \neq 0} (s_i - k + r_i) \ldots (s_i - k + 1) \prod_{j=2}^{q} \psi(N[\sigma_1(j),j] \ldots N[\sigma_k(j),j]) \prod_i X_i^{s_i - k}$$

$= f_k(N) \prod_i X_i^{s_i - k}$

□

Ce théorème nous donne une nouvelle expression pour f_k :
Proposition

$f_k(N(u,v)) =$

$$\sum_{\sigma_1,\ldots,\sigma_k \in S_q} \varepsilon(\sigma_1)\ldots\varepsilon(\sigma_k) \prod_{j=1}^{q} \psi(N[\sigma_1(j),j]\ldots N[\sigma_k(j),j]).$$

Remarquons alors que le calcul de cette fonction ne dépend pas du premier terme λ_1 de $\lambda = (\lambda_1, k, \ldots, k)$. La plus petite valeur possible pour λ_1 est k (car λ doit être une partition, il faut donc $\lambda_1 \geq k$) aussi dirons-nous que f_k est la fonction harmonique associée au module $\underbrace{[k,\ldots,k]}_{q}$.
Par ailleurs l'expression de la proposition prouve que f_k est une fonction polynômiale en les indéterminées $N[i,j]$ qui peut bien sûr être calculée pour n'importe quel $N = N(u,v)$. Dans ce qui suit nous légitimons davantage l'extension de ce calcul.
Nous avons vu en 1.4 que l'opérateur θ_{T_j} correspond à l'opérateur ψ de [8] ou $\tilde{}$ de [1] dans le cas binaire. Et $\theta_{T_j}(\varepsilon_{H_x}.e_{t_i})$ (cf. 9) est correctement défini, même si T_j n'a pas la même composition que x : $F_{T_i,T_j}(x,y)$ calcule combien de fois un mot y (de même composition que T_j) apparaît dans $\theta_{T_j}(\varepsilon_{H_x}.e_{t_i})$. Il est en fait possible d'adapter la preuve du théorème 10 : la formule est encore valide et les termes s_k qui apparaissent dans la définition 13 correspondent à la composition de x (ou de T_i).
Notons que ce second cas particulier est évidemment une généralisation du précédent puisque dans le cas binaire toute partition s'écrit (λ_1, k). Du coup on en déduit une expression plus simple des polynômes $H_{k,T}(u)$ de [1].
Rappelons la décomposition :

$$\mathbb{C}[X_{(n-w,w)}] \simeq \bigoplus_{k \leq w} [n-k,k].$$

Soient T et u deux mots de poids quelconque, nous avons :

$$N(T,u) = \begin{pmatrix} n - 2w + |T \cap u| & |u| - |T \cap u| \\ |T| - |T \cap u| & |T \cap u| \end{pmatrix}$$

Posons $t = \underbrace{111 \quad \ldots 1 \quad 222 \ldots 2}_{k}$

La fonction harmonique peut être calculée grâce à :

$$F_k(T,u) = F_{t,t}(T,u) = \sum_{i=0}^{k} (-1)^i \frac{\binom{|T\cap u|}{k-i}\binom{|u|-|T\cap u|}{i}}{\binom{|T|}{k-i}\binom{n-|T|}{i}} \binom{k}{i}$$

Et en fait $F_k(T,.)$ correspond au polynôme $H_{k,T}(u)$ de [1] :

$$H_{k,T}(u) = m_k F_k(T,u)$$

avec $m_k = \binom{n}{k} - \binom{n}{k-1}$.

Deuxième partie

Schémas d'association, designs

Chapitre 3

Schémas d'association

3.1 Définition

Soit X un ensemble fini (de points), de cardinal supérieur ou égal à deux. Pour n entier ≥ 1, considérons un ensemble $\mathcal{R} = \{\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_n\}$ de $n+1$ relations binaires non vides $\mathcal{R}_i$ sur X, formant une partition du produit cartésien X^2.

Définition 16 *On dit que $(X, \mathcal{R})$ est un schéma d'association à n classes si :*

a) $\mathcal{R}_0$ est la diagonale,

b) Pour tout i dans $\{0, 1, \ldots, n\}$ la relation définie par :

$\mathcal{R}_i^{\cup} = \{(x, y) \in X^2 : (y, x) \in \mathcal{R}_i\}$ est dans $\mathcal{R}$,

c) Il existe des entiers $p_{i,j}^k$, appelés nombres intersections, vérifiant $p_{i,j}^k = p_{j,i}^k$, et tels que pour tout couple $(x, y) \in \mathcal{R}_k$, le nombre de points $z \in X$ tels que $(x, z) \in \mathcal{R}_i$ et $(z, y) \in \mathcal{R}_j$ est constant (égal à $p_{i,j}^k$), pour tout i, j, k dans $\{0, 1, \ldots, n\}$.

La condition b) induit sur $\{0, 1, \ldots, n\}$ une application $i \mapsto i^{\sigma}$ définie par $\mathcal{R}_{i^{\sigma}} = \mathcal{R}_i^{\cup}$. Le nombre $p_{i,i^{\sigma}}^0$ se note v_i et s'appelle la *valence* du graphe $(X, \mathcal{R}_i)$. Il compte les points $z \in X$ vérifiant $(x, z) \in \mathcal{R}_i$, pour tout $x \in X$. Bien sûr, $v_{i^{\sigma}} = v_i$ et $\sum_{i=0}^{n} v_i = |X|$. Un SA est dit *symétrique* si les relations $\mathcal{R}_i$ sont symétriques. Un SA $(X, \mathcal{R})$ peut être vu comme un espace X muni d'une fonction $\partial_{\mathcal{R}} : X^2 \to \{0, 1, \ldots, n\}$ définie par :

$$\partial_{\mathcal{R}}(x, y) = i \text{ ssi } (x, y) \in \mathcal{R}_i.$$

Dans le cas symétrique cette fonction a, en particulier, les propriétés $\partial_{\mathcal{R}}(x, y) = 0$ ssi $x = y$ et $\partial_{\mathcal{R}}(x, y) = \partial_{\mathcal{R}}(y, x)$, mais ne satisfait pas, en général, l'inégalité triangulaire et n'est donc pas une distance.

Remarquons enfin que les axiomes de SA peuvent être diversement modifiés ; ainsi si l'on supprime l'hypothèse $p_{i,j}^k = p_{j,i}^k$ on obtient ce qu'on appelle en théorie des groupes une *configuration cohérente homogène* ; par ailleurs, beaucoup d'auteurs ne considèrent que les SA symétriques, car la plupart des SA intervenant en théorie des codes le sont.

3.2 Exemples

Schéma de Hamming

Soient $\mathcal{F} = \{\alpha_0, \ldots, \alpha_{q-1}\}$ un alphabet fini (i.e. un ensemble fini dont les éléments sont appelés des *symboles*) de cardinal $q \geq 2$, $X = \mathcal{F}^n$ et $\partial_H : X^2 \to \{0, 1, \ldots, n\}$ la distance de Hamming définie par :

$$\partial_H(x, y) \stackrel{déf}{=} |\{j \in \{0, 1, \ldots, n\}, x_j \neq y_j\}|,$$

alors $(X, \mathcal{R})$ (avec $\partial_{\mathcal{R}}(x, y) = \partial_H(x, y)$) est un SA symétrique à n classes, appelé *schéma de Hamming* et noté H_q^n. Les éléments de X sont souvent appelés les *mots* du schéma ; n est leur *longueur*. Le poids d'un mot x est défini par la fonction w_H : $w_H(x) = |\{j \in \{0, 1, \ldots, n\} : x_j \neq \alpha_0\}|$ qu'on appelle *poids de Hamming*. Remarquons qu'on peut toujours identifier $\mathcal{F}$ à $\mathbb{Z}/q\mathbb{Z}$; dès lors $\alpha_0 = 0$ et : $\partial_H(x, y) = w_H(x - y)$. Enfin dans le cas où q est puissance d'un premier on peut aussi identifier $\mathcal{F}$ à un corps fini.

Schéma de Johnson

Soit X l'ensemble des mots de H_2^v de poids n fixé, avec $1 \leq n \leq \lfloor v/2 \rfloor$. Pour $i \in \{0, 1, \ldots, n\}$ posons

$$\mathcal{R}_i = \{(x, y) \in X^2 : \partial_H(x, y) = 2i\}$$

et

$$\mathcal{R} = \{\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_n\},$$

alors $(X, \mathcal{R})$ est un SA symétrique à n classes appelé *schéma de Johnson* et noté J_n^v. On peut le voir comme un "sous-schéma" de H_2^v constitué uniquement des mots de poids n. Si l'on identifie X aux parties d'un ensemble V à v éléments, on obtient un SA sur l'ensemble des parties de V ; et pour $A, B \subseteq V$ on a :

$$A\mathcal{R}_i B \Leftrightarrow |A \cap B| = v - i.$$

Schéma de Johnson non binaire

Si l'on étend la définition précédente à H_q^v on n'obtient pas en général de SA, comme le montre l'exemple suivant ; on prend :

$$\mathcal{F} = \{0, 1, 2\},\ v = 3,\ n = 2,\ x = (1, 1, 0).$$

Les mots à distance 2 de x ont un coefficient nul et une seule coordonnée commune à x ; on trouve :

$$(2, 2, 0), (1, 0, 1), (1, 0, 2), (0, 1, 1), (0, 1, 2).$$

Prenons $y = (2, 2, 0)$; tous les mots de la liste précédente sont à distance trois de y donc $p^2_{2,2}$ devrait être égal à 0. Prenons $y = (1, 0, 1)$, le mot $(0, 1, 1)$ est à distance deux de y donc $p^2_{2,2}$ devrait être égal à 1. Absurde.
Toutefois il est possible de raffiner les $\mathcal{R}_i$ afin d'obtenir un SA ; posons $e(x, y) = |\{i : x_i = y_i \neq \alpha_0\}|$ et $n(x, y) = |\{i : x_i \neq \alpha_0, y_i \neq \alpha_0\}|$ et définissons $\mathcal{R}_{i,j}$ sur X par :

$$\mathcal{R}_{i,j} = \{(x, y) \in X^2 : e(x, y) = n - i, n(x, y) = n - j\}).$$

Comme on le verra au paragraphe 3.4 ces relations induisent sur X une structure de SA : c'est le *schéma de Johnson non binaire* ([27]).

Schéma de composition

Plaçons nous dans le cas où $\mathcal{F} = \{\alpha_0, \ldots, \alpha_{q-1}\}$ est un groupe abélien. Pour mettre en valeur cette propriété on note $\mathbb{F}$ à la place de $\mathcal{F}$; on pose $X = \mathbb{F}^v$. Par définition, la composition de $x \in X$ est le q-uplet (entier) $(s_0(x), \ldots, s_{q-1}(x))$ où : $s_l(x) = |\{j \in \{1, \ldots, v\} : x_j = \alpha_l\}|$. Soit alors s une composition fixée ; on définit un ensemble $\mathcal{R}$ de relations binaires $\mathcal{R}_s$ où $\mathcal{R}_s$ est l'ensemble des (x, y) tels que la composition de $x - y$ soit s. Alors $(X, \mathcal{R})$ est un SA non symétrique appelé *schéma de composition* ; on l'appelle aussi parfois *schéma de Hecke*.

3.3 Algèbre de Bose-Mesner

Il est d'usage d'associer à une relation $\mathcal{R}$ sur un ensemble fini X sa matrice $\mathcal{D}$; c'est une matrice indexée sur $X \times X$ et définie par $\mathcal{D}_{x,y} = 1$ ou 0 selon que $x\mathcal{R}y$ ou non. Ainsi,

-la matrice de la relation d'égalité (i.e. la diagonale) est l'identité I,

-la matrice d'une relation symétrique est symétrique,

-la matrice de la relation $X \times X$ est la matrice J dont tous les coefficients égalent 1.
Dans ce qui suit nous noterons indifféremment $\mathcal{D}_{x,y}$ ou $\mathcal{D}(x,y)$ le $(x,y)^{ième}$ terme de $\mathcal{D}$.

Définition 17 *Soit $(X, \mathcal{R})$ un SA à n classes. On appelle algèbre de Bose-Mesner de $(X, \mathcal{R})$ et on note $\mathcal{A}$ le $\mathbb{C}$-espace vectoriel engendré par les matrices D_i des relations $\mathcal{R}_i$.*

Ces matrices s'appellent les *matrices d'adjacence* du SA. Remarquons que comme $\mathcal{R}$ est une partition de X^2, les D_i sont linéairement indépendantes et l'axiome a) montre que $\mathcal{A}$ contient I :

$$dim\ \mathcal{A} = n+1,\ D_0 = I,\ D_0 + D_1 + \ldots + D_n = J;$$

l'axiome b) montre que $\mathcal{A}$ est stable par transposition et les générateurs de $\mathcal{A}$ étant à coefficients réels, $\mathcal{A}$ est stable par conjugaison, donc stable par passage à l'adjoint : $A \mapsto A^*$. Enfin la condition c) montre que $\mathcal{A}$ est stable par multiplication :

$$D_i D_j = \sum_{k=0}^{n} p_{i,j}^k D_k = D_j D_i.$$

Ainsi $\mathcal{A}$ est une $\mathbb{C}$-algèbre commutative (d'où la terminologie !). Si le SA est symétrique, les D_i sont symétriques et commutent deux à deux donc sont simultanément diagonalisables sur $\mathbb{R}$ et l'on pourra se restreindre au $\mathbb{R}$-espace vectoriel qu'elles engendrent.

Propriétés

Dans tous les cas $\mathcal{A}$ est formée de matrices normales et commutant deux à deux. Il existe donc une matrice unitaire S d'ordre $|X|$ qui diagonalise les éléments de $\mathcal{A}$ ($\mathcal{A}$ est semi-simple). On sait qu'alors $\mathcal{A}$ possède une unique base de matrices idempotentes $E_0, E_1, \ldots, E_n$ mutuellement orthogonales :

$$E_k E_l = \delta_{k,l} E_k.$$

En particulier $E_0 = |X|^{-1} J$.
On notera m_k le rang de E_k et les nombres m_k seront appelés les *multiplicités* du SA.
Les E_i étant idempotentes ce sont des matrices de projection : leurs valeurs propres sont 0 ou 1 et $Tr\ E_k = rg\ E_k = m_k$.
En outre S étant unitaire on a la relation $E_k^* = E_k$ qui montre que E_k est

la matrice de la projection orthogonale sur $V_k \stackrel{déf}{=} Im\ E_k$ (espace engendré par les colonnes de E_k) qui est donc le sous-espace propre attaché à la valeur propre 1.
Par ailleurs ce qui précède montre que les E_i sont hermitienne positives ; ce fait aura d'importantes conséquences par la suite.
Le théorème qui suit relie S aux E_k.

Théorème 12 *Il existe une partition $\cup_{k=0}^{n} X_k$ de X telle que si S_k est la restriction de S à $X \times X_k$, alors :*

$$|X|E_k = S_k S_k^*.$$

p-nombres et q-nombres

Les *p-nombres* $p_i(k)$ (resp. les *q-nombres* $q_k(i)$) sont définis à partir de l'écriture des D_i (resp. des E_k) dans la base des E_k (resp. des D_i) :

$$D_i = \sum_{k=0}^{n} p_i(k) E_k$$

$$|X|E_k = \sum_{i=0}^{n} q_k(i) D_i.$$

Ces nombres jouent un rôle important dans la théorie. Ils conduisent naturellement à considérer les matrices P et Q définies par : $P_{k,i} = p_i(k)$ et $Q_{i,k} = q_k(i)$.
Ce sont des matrices de changement de base. Ainsi :

$$PQ = QP = |X|Id.$$

Toute colonne de P (resp. de Q) peut être vue comme un élément de l'espace vectoriel des fonctions de $\{0, 1, \ldots, n\}$ dans $\mathbb{C}$. Or cet espace est de dimension $n+1$ donc les fonctions précédentes, que l'on appelle les p-fonctions (resp. les q-fonctions), forment une base de cet espace.
La relation :

$$D_i E_l = \sum_{k=0}^{n} p_i(k) E_k E_l = p_i(l) E_l$$

montre que les colonnes de E_l sont vecteurs propres (de D_i) pour la valeur propre $p_i(l)$. En particulier $D_i E_0 = p_i(0) E_0$ avec $E_0 = |X|^{-1} J$ et $p_i(0)$ est la

valence de D_i.
Par ailleurs,

$$m_k = Tr\ E_k = \frac{1}{|X|}\sum_{i=0}^{n} q_k(i) Tr\ D_i$$

or $D_0 = I$ et les $\mathcal{R}_i$ formant une partition de X^2, la diagonale de D_i est nulle pour $i \geq 1$ ($Tr\ D_i = 0$) et ainsi : $m_k = q_k(0)$.
Dans la mesure où les $\mathcal{R}_i$ forment une partition de X^2, pour $(x, y) \in X^2$ un seul terme (au plus) dans $\sum_{i=0}^{n} q_k(i) D_i(x, y)$ est non nul ; d'où :

$$|X| E_k(x, y) = q_k(\partial_{\mathcal{R}}(x, y)).$$

En outre les p-fonctions p_i et les q-fonctions q_k satisfont des relations d'orthogonalité :

Théorème 13

$$\sum_{k=0}^{n} m_k \overline{p_i(k)} p_j(k) = |X| v_i \delta_{i,j}$$

$$\sum_{i=0}^{n} v_i \overline{q_k(i)} q_l(i) = |X| m_k \delta_{k,l}.$$

Enfin, une formule relie les p-nombres et les q-nombres :

Théorème 14

$$m_k \overline{p_i(k)} = v_i q_k(i).$$

3.4 SA provenant de groupes

Soit G un groupe agissant transitivement sur un ensemble X. Il induit une partition $\mathcal{R} = \{\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_n\}$ de X^2 en orbites $\mathcal{R}_i$ (par définition $\mathcal{R}_i$ est l'ensemble des (x_i^g, y_i^g) pour $(x_i, y_i) \in X^2$ fixé, g parcourant G). On obtient une structure vérifiant les axiomes a), b), c) de SA sauf éventuellement la condition $p_{i,j}^k = p_{j,i}^k$, c'est-à-dire une configuration cohérente homogène ; a) et b) ne posant pas de problèmes, montrons c) : soient x, y tels que $x\mathcal{R}_k y$ et soit $Z \stackrel{déf}{=} \{z\ tels\ que\ x\mathcal{R}_i z\ et\ z\mathcal{R}_j y\}$. Soient x', y' tels que $x'\mathcal{R}_k y'$, par définition il existe g tel que $x' = x^g, y' = y^g$ et il vient $Z^g \stackrel{déf}{=} \{z^g, z \in Z\} = \{z' \in Z, x'\mathcal{R}_i z'\ et\ z'\mathcal{R}_j y'\}$ et bien sûr $|Z| = |Z^g|$.
Certains SA peuvent ainsi être obtenus à partir d'un groupe ; donnons quelques exemples.

Schéma de Hamming

On pose $\mathcal{F} = \{\alpha_0, \ldots, \alpha_{q-1}\}$, $x \in \mathcal{F}^v$ et G le groupe engendré par :

i) une permutation sur les n coordonnées,

ii) pour chaque coordonnée une permutation sur les q symboles de l'alphabet.

Ce groupe a pour ordre $n!(q!)^n$ et est transitif sur X. Les orbites sur X^2 sont constituées des mots à distance fixée, elles correspondent donc aux relations du schéma de Hamming. Ces relations étant symétrique on en déduit que $p^k_{i,j} = p^k_{j,i}$ et le schéma de Hamming est donc bien un SA.

Schéma de Johnson

Soit X l'ensemble des mots de H_2^v de poids n ; le groupe symétrique S_v agit transitivement sur X et induit une structure de SA (les relations sont encore symétriques) correspondant au schéma de Johnson.

Schéma de composition

Soit $(\mathbb{F}, +)$ un groupe abélien à q éléments ; on pose $X = \mathbb{F}^n$ et on note G le groupe (de permutations) engendré par :

i) une permutation σ sur les n coordonnées : $\sigma(x) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$,

ii) pour chaque coordonnée, une translation t_i : $t(x) = t + x = (x_1 + t_1, \ldots, x_n + t_n)$

Soit s une composition donnée et soit $(x, y) \in \mathcal{R}_s$. Alors $s(\sigma(x) - \sigma(y)) = s(\sigma(x - y)) = s(x - y) = s$ et $s((t + x) - (t + y)) = s(x - y) = s$ donc $\sigma(x)\mathcal{R}_s\sigma(y)$ et $(t + x)\mathcal{R}_s(t + y)$. Tout $g \in G$ se décomposant en produit de permutations (de coordonnées, i.e. de type σ) et de translations, il vient : $x^g \mathcal{R}_s y^g \ \forall g \in G$.

Soient $(x, y) \in \mathcal{R}_s$ et $(x', y') \in \mathcal{R}_s$. Alors il existe σ telle que $\sigma(x - y) = \sigma(x' - y')$ (en effet $x' - y'$ et $x - y$ ont même composition, i.e. sont formés des mêmes termes, à une permutation près). Ensuite : $\sigma(x) - \sigma(y) = x' - y' = s$ d'où : $y' - \sigma(y) = x' - \sigma(x)$, différence que l'on pose égale à t. On a donc : $(t \circ \sigma)(x) = x', (t \circ \sigma)(y) = y'$ et $t \circ \sigma$ est clairement un élément de G. D'où :

$$\forall (x, y) \in \mathcal{R}_s, \mathcal{R}_s = \{(x^g, y^g), g \in G\}.$$

Comme par ailleurs G agit transitivement sur X (partant de x on atteint y en translatant de $y - x$), on en déduit que le schéma de composition provient de l'action de G.

3.5 Liens avec la représentation des groupes

Supposons qu'un SA $(X, \mathcal{R})$ soit issu d'un groupe G. Il est clair qu'alors l'espace $V_k = Im\ E_k$ vu en est G-invariant ; c'est donc une représentation du groupe G. L'algèbre de Bose-Mesner $\mathcal{A}$ étant semi-simple, on en déduit le :

Théorème 15 *Soit G un groupe agissant transitivement sur un ensemble X, il y a équivalence entre les 2 propriétés suivantes :*
- *$(X, \mathcal{R})$ est un SA*
- *les multiplicités des modules irréductibles qui apparaissent dans la décomposition de la représentation $\mathbb{C}[X]$ sont toutes égales à un :*

$$\mathbb{C}[X] = \bigoplus_k V_k$$

Nous avons donc affaire en fait à un *espace symétrique* ou encore à une paire de Gelfand (cf. [18]) ; soit H le stabilisateur d'un élément $x \in X$ nous avons : $X \simeq G/H$. Il est alors naturel d'étudier dans ce cadre les fonctions harmoniques. La multiplicité étant un il n'y a en fait qu'une fonction harmonique (à multiplication par un scalaire près) par composante V_k et la relation $|X|E_k(x, y) = q_k(\partial_{\mathcal{R}}(x, y))$ vu en 3.3 montre que les q-nombres q_k correspondent en fait à ces fonctions harmoniques.
Considérons à présent les orbites de X_s^2 sous l'action de S_n ; on obtient une configuration cohérente homogène qui n'est pas un SA : en effet, en vertu du théorème 8, les orbites correspondent à des ensembles de couples (x, y) ayant même $N(x, y)$. Or cette matrice n'est pas symétrique en général ; par exemple pour $x = (1, 1, 2, 3)$ et $y = (1, 3, 1, 2)$ on a $N(x, y) = \begin{pmatrix} 101 \\ 100 \\ 001 \end{pmatrix}$. On en déduit que la condition $p_{i,j}^k = p_{j,i}^k$ n'est pas réalisée. Cela étant dit, dans le cas particulier $q = 2$ les matrices sont symétriques, d'où une structure de SA qui est en fait le schéma de Johnson (notons que le schéma de Johnson non-binaire ne correspond pas à notre situation). Les fonctions harmoniques vues au chapitre 2 correspondent donc en fait aux "q-nombres" de cette configuration.
Notons que les classes de cette configuration sont en bijection avec l'ensemble $\mathcal{N}_s$ des matrices à coefficients entiers dont la somme des termes de la $i^{ème}$ ligne = la somme des termes de la $i^{ème}$ colonne $= s_i$. Soit $N \in \mathcal{N}_s$ une telle matrice, posons pour $i, j = 1, \ldots, q$:

$$N'_{i,j} = \sum_{l=1}^{j-1} N[i, l].$$

Ainsi, pour tout i : $N'_{i,0} = 0$, $N'_{i,1} = N[i,1]$, $N'_{i,q} = s_i - N[i,q]$. Le nombre d'éléments d'une classe $\mathcal{R}_N$ est alors donné par la formule :

$$|\mathcal{R}_N| = \prod_{i=1}^{q} \prod_{j=1}^{q-1} \binom{N[i,j]}{s_i - N'_{i,j}}.$$

Si l'on pose à présent $s'_i = \sum_{l=1}^{i-1} s_l$ le nombre d'éléments de X_s est donné par la formule :

$$|X_s| = \prod_{i=1}^{q-1} \binom{n - s'_i}{s_i}$$

et l'on a bien sûr la relation :

$$\sum_{N \in \mathcal{N}_s} |\mathcal{R}_N| = |X_s|^2.$$

Chapitre 4

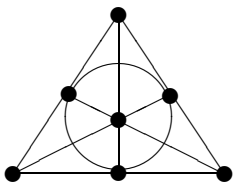
Designs

4.1 Designs classiques

Soit X un ensemble fini (de *points*) et $\mathcal{B}$ une famille de parties (appelées *blocs*) de X.

Définition 18 *On dit que $(X, \mathcal{B})$ est un t-(v, k, λ) design ou encore un t-design combinatoire si :*
- $|X| = v$,
- *les blocs de $\mathcal{B}$ sont tous de taille k (i.e. de cardinal k),*
- *toute partie de X à t éléments est contenue dans exactement λ blocs.*

Bien sûr l'ensemble des parties à k éléments de X est un exemple (trivial) de k-design ; en pratique on cherche toujours à obtenir des designs contenant le moins possible de blocs.
Le nombre λ de la définition est appelé le *paramètre du design* ; si il vaut 1 on dit que le design est un *système de Steiner*.
Exemple : considérons le graphe ci-après :



Plan de Fano

Nous prenons pour X l'ensemble des 7 sommets du graphe. Considérons à

présent les 6 droites de la figure : elles définissent 6 sous-ensemble de trois points ; ajoutons le sous-ensemble des trois points situés sur le cercle : nous obtenons un ensemble $\mathcal{B}$ de 7 parties de X à trois éléments et il est facile de voir que deux points quelconque définissent une unique droite (ou le cercle), ainsi $\mathcal{B}$ est-il un 2-$(7, 7, 1)$ design. C'est donc un système de Steiner, on l'appelle *plan de Fano*. Nous verrons dans la partie consacrée aux codes comment trouver assez facilement des exemples intéressants de designs.

Théorème 16 *Soit $t > 1$ un entier. Un t design combinatoire est aussi un $t - 1$ design combinatoire.*

Ce théorème apparaîtra plus tard comme un simple corollaire au théorème 21. Le plus grand entier t tel qu'un design soit un t-design est appelé la *force* du design.

Généralisation : designs colorés

On a généralisé de diverses manières la notion de design ; nous donnons ici l'exemple des designs colorés dû à A. Bonnecaze, E. Rainset P. Solé ([2]) Une *structure d'incidence colorée* Σ est un ensemble $\mathcal{P}$ de "points", un ensemble $\mathcal{B}$ de "blocs" , un ensemble $\mathcal{C}$ de "couleurs" auxquels on adjoint une fonction :

$$\rho : \mathcal{P} \times \mathcal{B} \to \mathcal{C};$$

nous dirons que $B \in \mathcal{B}$ est de couleur $\rho(P, B)$ en $P \in \mathcal{P}$. Nous dirons qu'une structure d'incidence colorée est *uniforme* si il existe une fonction $n : \mathcal{C} \to \mathbb{Z}$ appelée *palette* telle que pour chaque couleur $C \in \mathcal{C}$ tous les blocs utilisent $n(C)$ fois la couleur C. Enfin une structure d'incidence colorée est dite *simple* si deux blocs ne "colorient" jamais Σ de la même façon.

Définition 19 *Une structure d'incidence colorée simple et uniforme est appelée un t-design coloré si, pour n'importe quel multi-ensemble de t couleurs (répétitions autorisées), il existe un nombre λ tel que pour tout choix de t-points, exactement λ blocs utilisent cet ensemble de couleurs pour ces points. Un t-design coloré sera dit fort si les couleurs et les points sont ordonnés.*

Un t-design classique est un t-design coloré fort à deux couleurs ; mais en général un t-design coloré n'est pas fort. Etant donné un t-design coloré on peut décider d'identifier les couleurs : appelons cette opération "blanchiment", on voit qu'après blanchiment un t-design coloré demeure un t-design.
A. Bonnecaze, E. Rains et P. Solé ont prouvé l'analogue du théorème 16 :

Théorème 17 *Un t-design coloré (fort) est aussi un $t-1$-design coloré (fort).*

Nous reviendrons sur les designs colorés dans le paragraphe 4.4 et nous en donnerons des exemples non triviaux dans la troisième partie (paragraphe 5.4).

4.2 Codes et designs dans les SA

Dans ce paragraphe on définit des codes et des designs "généralisés". Le lien avec les designs classiques évoqués dans la section precédente est fait grâce au théorème 20 : ils vont correspondre aux designs du schéma de Johnson.

Dans tout ce qui suit on se place dans un SA à n classes $(X, \mathcal{R})$ fixé ; on appellera *code* Y tout sous ensemble non vide Y de X. On notera $\mathbf{Y}$ le vecteur caractéristique de Y : il est indexé sur X et est défini par $\mathbf{Y}_x = 1$ ou 0 selon que $x \in \mathbf{Y}$ ou non.

Définition 20 *La distribution interne d'un code Y est le $(n+1)$-uplet $\boldsymbol{a} = (a_i)_{i=0}^n$ où a_i est défini par :*

$$a_i = a_i(Y) \stackrel{déf}{=} \frac{1}{|Y|}|Y^2 \cap \mathcal{R}_i|.$$

Définition 21 *La distribution externe d'un code Y est la matrice M indexée sur $X \times \{0, \ldots, n\}$ et définie par :*

$$M_{x,i} = |\{y \in Y, (x,y) \in \mathcal{R}_i\}|.$$

Les codes intéressants sont souvent ceux dont les distances ne peuvent prendre que certaines valeurs (typiquement, les codes dont la distance minimale est supérieure à une borne donnée). D'où la définition suivante :

Définition 22 *Soit D un sous ensemble de $\{1, \ldots, n\}$. On appelle D-code dans $(X, \mathcal{R})$ tout code Y dont la distribution interne vérifie :*

$$a_i(Y) = 0 \ \forall i \in \{1, \ldots, n\} \setminus D.$$

Cela signifie que tout couple de points distincts de Y appartient à $\cup_{i \in D} \mathcal{R}_i$. Pour aborder les designs nous avons besoin d'une définition supplémentaire :

Définition 23 *La Q-transformée d'un* $(n+1)$*-uplet* $\boldsymbol{a} = (a_i)_{i=0}^n$ *est le* $(n+1)$*-uplet* $\boldsymbol{a'} = (a'_k)_{k=0}^n = \boldsymbol{a}Q$ *:*

$$a'_k = \sum_{i=0}^{n} a_i q_k(i).$$

Remarquons que : $|Y|a'_k(Y) = |X|\mathbf{Y}^t E_k \mathbf{Y}$ car :

$$|X|\mathbf{Y}E_k^t\mathbf{Y} = \sum_{x,y\in Y^2} q_k(\partial_{\mathcal{R}}(x,y)) = \sum_{i=0}^{n} q_k(i)|Y|a_i(Y) = |Y|a'_k(Y).$$

Notons alors que :

$$a'_k(Y) = 0 \Leftrightarrow \mathbf{Y}^t E_k \mathbf{Y} = 0 \Leftrightarrow \|E_k\mathbf{Y}\| = 0 \Leftrightarrow E_k\mathbf{Y} = 0.$$

Définition 24 *Soit* D *un sous ensemble de* $\{1,\ldots,n\}$*. Un code* Y *sera appelé un* D*-design si la* Q*-transformée de sa distribution interne vérifie :*

$$a'_k(Y) = 0 \ \forall k \in \{1,\ldots,n\} \setminus D$$

ou, de façon équivalente :

$$E_k\,\boldsymbol{Y} = 0 \ \forall k \in \{1,\ldots,n\} \setminus D.$$

Si d et t sont deux entiers tels que $1 \leq d \leq n$ et $0 \leq t \leq n-1$, on appellera *d-code* tout code Y pour lequel $a_i(Y) = 0$ si $i < d$ et *t-design* tout code pour lequel $a'_i(Y) = 0$ si $i \leq t$. Supposons que le SA soit issu d'un groupe G, on voit donc que Y sera un t-design si $\mathbf{Y}$ est orthogonal à certains G-modules irréductibles, plus précisément à t d'entre eux :

$$\mathbf{Y} \perp V_i \quad i = 1,\ldots,t.$$

On le voit, cette définition est de nature *algébrique*. Or la définition des designs est combinatoire. Bien sûr les deux définitions coïncident (cf. theorème 20) et en fait c'est un des succès de la théorie des SA de pouvoir offrir une approche algébrique à la notion combinatoire de design.
Enonçons maintenant un résultat simple, mais important : les *inégalités de Delsarte*.

Théorème 18 *Soit* Y *un code ; la* Q*-transformée de sa distribution interne vérifie :*

$$a'_k(Y) \geq 0 \ \forall k \in \{0,1,\ldots,n\}.$$

Plus précisément, si Q_k désigne la $k^{ième}$ colonne de Q :

$$Q^*M^tMQ = |X||Y| \begin{pmatrix} a'_0(Y) & & 0 \\ & \ddots & \\ 0 & & a'_n(Y) \end{pmatrix} \Leftrightarrow \|MQ_k\|^2 = |X||Y|a'_k(Y).$$

Preuve :
rappelons que la matrice E_k est hermitienne et positive, on a donc bien $a'_k(Y)(= \mathbf{Y}^tE_k\mathbf{Y}|X||Y|^{-1}) \geq 0$. D'autre part, remarquons que :

$$M = [D_0\mathbf{Y} \ \dots \ D_n\mathbf{Y}], MQ = |X|[E_0\mathbf{Y} \ \dots \ E_n\mathbf{Y}]$$

et avec (2.1), on obtient l'expression voulue de Q^*M^tMQ :

$$|X|^2 \begin{pmatrix} \mathbf{Y}^tE_0\mathbf{Y} & & 0 \\ & \ddots & \\ 0 & & \mathbf{Y}^tE_n\mathbf{Y} \end{pmatrix} = |X||Y| \begin{pmatrix} a'_0(Y) & & 0 \\ & \ddots & \\ 0 & & a'_n(Y) \end{pmatrix}.$$

□

Une distribution étant elle aussi toujours positive, D-designs et D-codes apparaissent ainsi comme des objets duaux, satisfaisant des propriétés d'extrémalité (paramétrée par D) ; ces résultats, dûs à Delsarte ([7]), permettent de fonder, de façon naturelle, la théorie des codes et des designs dans le cadre des schémas d'association.
Notons que le théorème précédent a permis de déterminer ([29]) la borne exacte intervenant dans le théorème d'Erdös-Ko-Rado : soit $\mathcal{F}$ une famille de k-parties d'un ensemble à n éléments telle que 2 éléments quelconques de $\mathcal{F}$ se rencontrent toujours en au moins t points ; si $n \geq (t+1)(k-t+1)$ alors $|\mathcal{F}| \leq \binom{n-t}{k-t}$.

4.3 Exemple du schéma de Johnson J_n^v

Pour simplifier ce qui suit, on pose $\mathcal{F} = \{0,1\} = \mathbb{F}_2$.
Les mots de J_n^v sont binaires de poids n ($\leq v/2$) : on peut donc les identifier aux n-parties (i.e. aux parties à n éléments) d'un ensemble V à v éléments. Plus précisément, soit $V = \{1, 2, \dots, v\}$ et soit V_n l'ensemble des parties de V à n éléments. L'application $f : x \mapsto f(x) = \{p \in V, x_p = 1\}$ réalise une bijection de $\mathbb{F}_2^v$ sur l'ensemble des parties de V et de J_v^n sur V_n. Cela explique que le schéma de Johnson soit propice à l'étude de problèmes combinatoires.

p-nombres et q-nombres

Théorème 19 *Les valences et les multiplicités de J_n^v sont données par :*

$$v_i = \binom{n}{i}\binom{v-n}{i},$$

$$m_k = \binom{v}{k} - \binom{v}{k-1},$$

les p-nombres et les q-nombres de J_n^n sont donnés par :

$$p_i(k) = \sum_{j=0}^{i}(-1)^{i-j}\binom{n-j}{i-j}\binom{n-k}{j}\binom{v-n+j-k}{j}$$

$$q_k(i) = m_k \sum_{j=0}^{k}(-1)^j \frac{\binom{k}{j}\binom{v+1-k}{j}}{\binom{n}{j}\binom{v-n}{j}}\binom{i}{j}.$$

Les polynômes q_k sont appelés *polynômes de Hahn*

Designs

Théorème 20 *Soit t un entier $\leq n-1$. Les t-designs de J_n^v correspondent aux t-designs combinatoires de $V = \{1, 2, \ldots, v\}$.*

Preuve :
pour $i = 0, 1, \ldots, n$ posons :

$$C_i = \sum_{k=i}^{n}\binom{k}{i}D_{n-k}$$

où D_{n-k} désigne bien entendu la $(n-k)^{ième}$ matrice adjacente de J_n^v. Par définition C_i est une matrice de taille $\binom{v}{n} \times \binom{v}{n}$ indicée par les mots de J_v^n ; or, un couple $(x, y) \in \mathcal{R}_{n-k}$ ssi x et y coïncident en k termes, ce qui signifie que $f(x) \cap f(y)$ est une k-partie de V. Les $\mathcal{R}_{n-k}$ étant disjointes, on en déduit que $C_i(x, y)$ est le nombre de i-parties de $f(x) \cap f(y)$.
De plus avec la formule d'inversion de Pascal, il vient :

$$D_{n-k} = \sum_{r=k}^{n}\binom{r}{k}C_r$$

et les C_r sont une nouvelle base de $\mathcal{A}$.

Lemme *Les matrices $C_0, C_1, \ldots, C_n$ vérifient :*

$$C_r C_s = \sum_{t=0}^{min(r,s)} \binom{n-t}{r-t}\binom{n-t}{s-t}\binom{v-r-s}{v-n-t} C_i.$$

Preuve :
$C_i(x,y)$ se calcule de la façon suivante : pour $\gamma \in V_n$ on fait le produit du nombre de r-parties de $f(x) \cap \gamma$ par le nombre de s-parties de $\gamma \cap f(y)$ puis on somme sur les γ ; on peut donner une interprétation combinatoire de $C_i(x,y)$: c'est le nombre de triplets $(\alpha, \beta, \gamma) \in V_r \times V_s \times V_n$ vérifiant $\alpha \subseteq f(x), \beta \subseteq f(y), \alpha \cup \beta \subseteq \gamma$.

Afin de calculer cette quantité, fixons les valeurs de $|\alpha \cap f(y)|(= i)$ et de $|\alpha \cap \gamma|(= j)$; pour i et j fixés donc, on trouve le nombre de possibilités pour α : il faut en effet lui choisir $|\alpha \cap (f(y) \cap f(x))| = i$ éléments dans $f(y)$ $(f(y) \cap f(x)$ en fait) et $r - i$ dans les $n - u$ éléments restants de $f(x)$. D'où un premier terme :

$$\binom{u}{i}\binom{n-u}{r-i};$$

on procède de même pour β :

$$\binom{i}{j}\binom{n-i}{s-j}$$

et pour γ :

$$\binom{v-r-s+j}{n-r-s+j} = \binom{v-r-s+j}{v-n}.$$

Par ailleurs, la décomposition du polynôme $\binom{n-u}{r-i}\binom{u}{i}$ dans la base des $\binom{u}{t}$ est connue :

$$\binom{n-u}{r-i}\binom{u}{i} = \sum_{t=0}^{r}(-1)^{t-i}\binom{t}{i}\binom{n-t}{r-t}\binom{u}{t}$$

et on a : $\binom{u}{t} = C_t(x,y)$ pour $f(x) \cap f(y) \in V_u$. Donc $C_r C_s$ est combinaison linéaire de $C_0, C_1, \ldots, C_r$ et le coefficient correspondant à C_t est :

$$\binom{n-t}{r-t}\sum_{j=0}^{n}\binom{v-r-s+j}{v-n}\sum_{t=0}^{n}(-1)^{t-i}\binom{t}{i}\binom{i}{j}\binom{n-i}{s-j}$$

et en réutilisant (2.6) :

$$\binom{n-t}{r-t}\binom{n-t}{s-t}\sum_{t=0}^{n}(-1)^{j-t}\binom{t}{j}\binom{v-r-s+j}{v-n}$$

d'où l'on déduit la formule annoncée. □

Ce théorème montre que C_rC_s est combinaison linéaire de C_t, avec $t \leq r$. D'où une chaîne d'idéaux $\mathcal{A}_r \stackrel{déf}{=} Vect\{C_0, C_1, \ldots, C_r\}$ de dimension $r+1$ tels que :

$$\langle J \rangle = \mathcal{A}_0 \subset \mathcal{A}_1 \subset \ldots \subset \mathcal{A}_n = \mathcal{A}.$$

On sait alors que quitte à permuter les idempotents E_k, on peut supposer que $(E_0, E_1, \ldots, E_r)$ est une base de $\mathcal{A}_r$.
Soit N_i la matrice d'inclusion d'une i-partie de V dans une n-partie de V. Plus précisément, N_i est indexée par l'ensemble X des mots de J_n^v et par V_i, et l'on a $N_i(x, \alpha) = 1$ ou 0 selon que $\alpha \subseteq f(x)$ ou non. On constate qu'alors : $C_i = N_iN_i^t$.
Soit donc Y un t-design de J_n^v ; pour $k \leq t$ on a :

$$\mathbf{Y}^t E_k \mathbf{Y} = 0$$

et de plus, en désignant par $\mathbf{1}$ le vecteur qui a toutes ses coordonnées égales à 1 :

$$\mathbf{1}^t E_k \mathbf{1} = 0$$

pour $k \neq 0$ puisqu'alors $|X|E_kE_0 = E_kJ = 0$. En outre :

$$(\mathbf{Y} - \alpha\mathbf{1})^t E_0 (\mathbf{Y} - \alpha\mathbf{1}) = 0$$

pour α égal à : $|Y|/\binom{v}{n}$. De tout cela on déduit, en se rappelant que pour les $i \leq n$ $Vect\{N_0N_0^t, \ldots, N_iN_i^t\} = Vect\{E_0, \ldots, E_i\}$:

$$(\mathbf{Y} - \alpha\mathbf{1})^t N_t N_t^t (\mathbf{Y} - \alpha\mathbf{1})$$

c'est-à-dire $\mathbf{Y}^t N_t = \alpha\mathbf{1}^t N_t = \lambda\mathbf{1}^t$ pour un certain λ.
Or les coordonnées de $\mathbf{Y}N_t$ correspondent au nombre de n-parties de $f(Y)$ contenant une t-partie donnée. Ainsi $f(Y)$ est un t-design combinatoire. Réciproquement, un t-design combinatoire est un i-design combinatoire pour tout $i \leq t$; aussi en remontant le raisonnement précédent, on aboutit à $\mathbf{Y}^t E_i \mathbf{Y} = 0$ pour $i = 1, \ldots, t$ ce qui signifie que Y est un t-design de J_n^v. □

4.4 Designs généralisés

Dans cette section nous étudions la généralisation des designs combinatoires due à A. Bonnecaze, E. Rains, P. Solé (cf. [2]). Nous emploierons

librement les notations vues dans la première partie (paragraphe 1.2. Ainsi $\mathcal{F}_q = \{1, \ldots, q\}$ et le poids d'un mot $x \in \mathcal{F}_q^n$ est le nombre de ses coefficients égaux à 1. Nous aurons aussi besoin du *poids* $|s|$ d'une composition s : c'est par définition le poids de n'importe quel élément de composition s : $|s| = s_2 + \ldots + s_q$. Nous supposerons que s est une partition de n. Nous utiliserons enfin l'ordre suivant défini sur les mots de $X = \mathcal{F}_q^n$:

$$x \leq y \Leftrightarrow x_i = 1 \text{ ou } y_i \text{ pour } i = 1, \ldots, n$$

et nous dirons que y *couvre* x.

Définition 25 *Un ensemble de mots $\mathcal{B}$ de $\mathcal{F}_q^n$ est appelé un t-design (généralisé) si tous les mots de $\mathcal{B}$ ont même composition (disons s) et si pour toute composition τ telle que $|\tau| = t$ il existe un entier λ_τ tel que :*

$$\forall T \in X, \quad s(T) = \tau \Rightarrow |\{x \in \mathcal{B}, T \leq x\}| = \lambda_\tau.$$

Bien sûr cette définition correspond à la définition des t designs colorés forts. Appelons *blanchiment* l'application de $\mathcal{F}_q$ dans $\mathcal{F}_2$ qui remplace tout élément différent de 1 par "2". Après blanchiment un t-design est un t-design combinatoire classique. Nous savons grâce au théorème 20 que les designs combinatoires sont les designs du schéma de Johnson. Aussi peut-on se demander si les designs que nous venons d'introduire sont associés à un SA, qui serait la généralisation du schéma de Johnson. Le théorème qui suit répond à cette question.
Un design $\mathcal{B}$ étant un sous-ensemble de X_s nous noterons $f_\mathcal{B}$ son vecteur caractéristique :

$$f_\mathcal{B} = \sum_{x \in \mathcal{B}} x \in \mathbb{C}[X_s]$$

Par ailleurs rappelons que l'espace V_λ^s est par definition une composant isotypique (non irréductible en général !) de la décomposition :

$$\mathbb{C}[X_s] = \bigoplus_{\lambda \trianglerighteq s} V_\lambda^s$$

Théorème 21 *$\mathcal{B}$ est un t-design $\Leftrightarrow f_\mathcal{B} \perp V_\lambda^s \quad 0 < |\lambda| \leq t$*

Ainsi les designs généralisés sont-ils associés à la configuration cohérente homogène vue au paragraphe 3.5.
Notons qu'avec ce théorème il est clair qu'un un t-design est un $(t-1)$-design.
Au paragraphe 4.6 nous déduirons de ce théorème un algorithme pour tester si un ensemble donné est un design.

4.5 Preuve du théorème 21

Opérateurs d_s et d^s

Soit $i \in \{1, \ldots, q\}$ et soit $d_i : \mathbb{C}[X] \to \mathbb{C}[X]$ l'opérateur défini sur $X = \mathcal{F}_q^n$ par :

$$x = (x_1, x_2, \ldots, x_n) \mapsto \sum_{k, x_k = i} (x_1, x_2, \ldots, x'_k, \ldots, x_n)$$

avec $x'_k = 1$.
On étend alors d_i à $\mathbb{C}[X]$ par linéarité.
Exemple :

$$d_3(1,2,3,2,1,3) = (1,2,1,2,1,3) + (1,2,3,2,1,1)$$

Remarque : Si $x \in \mathbb{C}[X_{(s_1,s_2,\ldots,s_q)}]$ alors $d_i(x) \in \mathbb{C}[X_{(s_1+1,s_2,\ldots,s_i-1,\ldots,s_q)}]$ et si $s_i(x) = 0$ alors $d_i(x) = 0$.

Proposition *Les opérateurs d_i commutent : $d_i d_j = d_j d_i$. En outre ce sont des homomorphismes de S_n-module.*
La preuve est très simple et est laissée au lecteur. □

Soit $i \in \{1, \ldots, q\}$ et soit d^i l'opérateur défini par :

$$y = (y_1, y_2, \ldots, y_n) \mapsto \sum_{k, y_k = 1} (y_1, y_2, \ldots, y^*_k, \ldots, y_n)$$

avec $y^*_k = i$. d^i est ensuite étendu à tout $\mathbb{C}[X]$ par linéarité.

Remarque : Si $x \in \mathbb{C}[X_{(s_1,s_2,\ldots,s_q)}]$ alors $d^i(x) \in \mathbb{C}[X_{(s_1-1,s_2,\ldots,s_i+1,\ldots,s_q)}]$ et si $s_1(x) = 0$, alors $d^i(x) = 0$.

Proposition *L'opérateur d^i est l'adjoint de d_i.*
Preuve :
soient $x, y \in X$ il nous faut prouver :

$$\langle d_i(x), y \rangle = \langle x, d^i(y) \rangle$$

Si $i = 1$ le résultat est évident : $\langle d_i(x), y \rangle = s_1(x)\delta_{x,y} = \langle x, d^i(y) \rangle$ Nous supposerons donc : $i > 1$. Deux cas peuvent se produire : ou bien il existe un certain k tel que $(x_1, \ldots, x'_k, \ldots, x_n) = (y_1, \ldots, y_n)$, ou bien pour tout k $(x_1, \ldots, x'_k, \ldots, x_n) \neq y$.

- si il existe un certain k tel que $(x_1, \ldots, x'_k, \ldots, x_n) = (y_1, \ldots, y_n)$ nous avons alors $(x_1, \ldots, x'_l, \ldots, x_n) \neq (y_1, \ldots, y_n)$ pour tout $l \neq k$, d'où $\langle d_i(x), y\rangle = 1$. D'un autre côté $(x_1, \ldots, x_n) = (y_1, \ldots, y^*_k, \ldots, y_n)$ donc $\langle x, d^i(y)\rangle = 1$ et dans ce cas $\langle d_i(x), y\rangle = \langle x, d^i(y)\rangle$
- si, pour tout k $(x_1, \ldots, x'_k, \ldots, x_n) \neq (y_1, \ldots, y_n)$ alors $\langle d_i(x), y\rangle = 0$. Nous devons prouver que $\langle x, d^i(y)\rangle = 0$. Supposons $\langle x, d^i(y)\rangle \neq 0$: il existe un k tel que $(x_1, \ldots, x_n) = (y_1, \ldots, y^*_k, \ldots, y_n)$ d'où $y_k = 1, y^*_k = i = x_k \Rightarrow x'_k = 1$ et donc : $(x_1, \ldots, x'_k, \ldots, x_n) = (y_1, \ldots, y_n)$ ce qui est faux.

Ainsi avons-nous toujours $\langle d_i(x), y\rangle = \langle x, d^i y\rangle$. □

Les opérateurs d_i commutent et sont des S_n-homomorphismes. Il en va bien entendu de même pour leurs adjoints. Pour toute composition s nous noterons d_s l'opérateur $\underbrace{d_2 \ldots d_2}_{s_2}\underbrace{d_3 \ldots d_3}_{s_3} \ldots \underbrace{d_q \ldots d_q}_{s_q}$.
Nous noterons d^s son adjoint : $\underbrace{d^2 \ldots d^2}_{s_2}\underbrace{d^3 \ldots d^3}_{s_3} \ldots \underbrace{d^q \ldots d^q}_{s_q}$.

Première caractérisation des designs

Soit τ une composition telle que $\tau \leq s$: nous entendons par là que pour tout $i \geq 2$: $\tau_i \leq s_i$. Nous noterons $s - \tau$ la composition $(n + s_1 - \tau_1, s_2 - \tau_2, s_3 - \tau_3, \ldots, s_q - \tau_q)$. Il est facile de voir que $\tau \leq s$ implique $\tau \trianglerighteq s$. Si nous n'avons pas $\tau \leq s$ nous poserons : $d_{s-\tau} = d^{s-\tau} = 0$. Dans ce paragraphe nous prouvons le résultat suivant :

Proposition *$\mathcal{B}$ est un t-design si et seulement si pour toute composition τ de poids t, il existe un μ_τ tel que $d_{s-\tau} f_{\mathcal{B}} = \mu_\tau d^\tau(1, \ldots, 1)$* Preuve :

soit $x \in X$; $d_i(x)$ est la somme des mots y de composition $s - (0, \ldots, \overset{i}{1}, \ldots, 0)$ couverts par x. En fait $d_{s-\tau}(x)$ est la somme à un facteur scalaire près des mots de composition $s - (s - \tau) = \tau$ couverts par x car :

-tous les mots apparaissant dans $d_{s-\tau}(x)$ sont couverts par x, et leur composition est τ,

-si un mot de composition τ est couvert par x, il apparaît dans $d_{s-\tau}(x)$,

-enfin il est facile de prouver soit par un argument de symétrie, soit par récurrence que chaque mot de $d_{s-\tau}(x)$ apparaît avec le même coefficient $\prod_{i=2}^{q} c_i!$ lequel ne dépend pas de x.

Ainsi avons-nous :

$$d_{s-\tau}(f_{\mathcal{B}}) = \sum_{x \in \mathcal{B}} d_{s-\tau}(x) = \sum_{x \in \mathcal{B}} \sum_{T \leq x} T = \sum_{T} T \sum_{x \in \mathcal{B}, T \leq x} 1 = \sum_{T} |\{x \in \mathcal{B}, T \leq x\}| T$$

d'où l'on déduit la proposition. □

Une autre décomposition de $K_{\lambda s}[\lambda]$

Théorème 22 *Soit p un entier. Pour toute partition λ telle que $0 < |\lambda| \leq p$ on a :*

$$\sum_{|\tau|=p} d^{s-\tau}(V_\lambda^\tau) = V_\lambda^s$$

la somme étant faite sur toutes les compositions de poids p.

Preuve :
les opérateurs d_i et d^i correspondent à des opérateurs définis sur $\mathbb{C}[T_{\lambda s}]$ (cf. 1.2) que nous noterons encore d_i et d^i. Soient $t \in T_{\lambda\tau}, t' \in T'_{\lambda s}$ on a :

$$\mathbb{C}[X_\lambda] \xrightarrow{\theta_t} \mathbb{C}[X_\tau] \xrightarrow{d^{s-\tau}} \mathbb{C}[X_s]$$

$$\mathbb{C}[X_\lambda] \xrightarrow{\theta_{t'}} \mathbb{C}[X_s]$$

nous allons prouver que pour tout $t' \in T^s_{\lambda s}$ on peut trouver un tableau $t \in T_{\lambda\tau}$ (pas forcément semi-standard) et une composition τ de poids p tels que $\theta_{t'}$ soit égal à $d^{s-\tau} \circ \theta_t$ à un scalaire près.
Soit $t \in T_{\lambda\tau}$ dont tous les 1 sont dans la première ligne. Nous avons une première égalité :

$$d^i \circ \theta_t(\overline{t_\tau}) = d^i \sum_{T \sim t} T.$$

Remplaçons alors un seul 1 de t par un i et soit t^* le tableau obtenu ; $d^i t$ est une somme de tels tableaux. Nous avons une seconde égalité :

$$\theta_{t^*}(\overline{t_\tau}) = \sum_{T^* \sim t^*} T^*.$$

En fait θ_{t^*} est égal (à un scalaire près) à $d^i \circ \theta_t$ car :

- tous les T^* de la seconde égalité sont distincts,
- dans la première égalité tous les 1 de t sont dans sa première ligne ; donc d^i agit seulement sur la première ligne de T et, pour tout T, $d^i T$ est bien sûr une somme de $T^* \sim t^*$.
- De plus, tout T^* peut être obtenu à partir d'un T en appliquant d^i, et en fait ce T est nécessairement obtenu en remplaçant un i de la première ligne de T^* par un 1.

Finalement tout T^* apparaît dans la seconde égalité le même nombre de fois (ce nombre est 1 + le nombre de i dans la première ligne de t). Par récurrence on montre que θ_{t^*} est égal (à un scalaire près) à $d^{s-\tau} \circ \theta_t$, où t^* est obtenu en remplaçant $(s_1 - \tau_1)$ "1" de t par des "2", $(s_2 - \tau_2)$ "2" de t par des "3",etc.

A présent soit $t' \in T'_{\lambda s}$. Comme $|s| - p \leq \lambda_1 - s_1$ (car $p \geq |\lambda| \Rightarrow p \geq n - \lambda_1 = |s| + s_1 - \lambda_1$) et comme $\lambda_1 - s_1$ est le nombre de coefficients $\neq 1$ de la première ligne de t', il est possible d'en remplacer $|s| - p$ par des 1 : on obtient alors un nouveau tableau t''. Soit τ sa composition : $t'' \in T_{\lambda\tau}$ et tous ses 1 sont dans sa première ligne (car t' est semi-standard). Et nous avons : $\theta_{t'}$ est égal (à un scalaire près) à $d^{s-\tau} \circ \theta_{t''}$. Et bien sûr : $|\tau| = |s| - (|s| - p) = p$. Donc :

$$\sum_{t' \in T'_{\lambda s}} \theta_{t'}([\lambda]) \subset \sum_{|\tau|=p} d^{s-\tau} \sum_{t \in T_{\lambda\tau}} \theta_t([\lambda])$$

c'est-à-dire :

$$V_\lambda^s \subset \sum_{|\tau|=p} d^{s-\tau}(V_\lambda^\tau)$$

et la proposition suit car l'autre inclusion est immédiate. □

4.6 Application

Un premier intérêt du théorème 21 est qu'il remplace la définition combinatoire des designs colorés par une définition algébrique ; de fait il précise dans quelle mesure les designs colorés sont les designs d'un "schéma d'association" (configuration cohérente homogène en fait). Mais ce théorème présente un autre intérêt : en effet il permet d'écrire, grâce aux fonctions harmoniques explicitées dans la première partie, un algorithme (non trivial) pour savoir si un ensemble est un design (généralisé).
L'algorithme en question est fourni par le résultat suivant.

Théorème 23 *Soit $\mathcal{B}$ est un sous-ensemble de X_s, on a :*

$$f_{\mathcal{B}} \perp V_\lambda^s \Leftrightarrow \sum_{y \in \mathcal{B}} F(x, y) = 0 \quad \forall x \in \mathcal{B}, \forall F \in \mathcal{F}_\lambda$$

où $\mathcal{F}_\lambda$ désigne une base de fonctions harmoniques.

Preuve :
soit $P_{\lambda s}$ la matrice (indicée sur X_s) de la projection orthogonale sur le sous-espace V_λ^s de $\mathbb{C}[X_s]$ dans la base X_s. Prouvons d'abord que $P_{\lambda s}$ est une fonction harmonique.

Si Λ est la matrice de n'importe qu'elle base orthonormée de V_λ^s dans la base X_s nous avons :

$$P_{\lambda s} = \Lambda\Lambda^*$$

avec $\Lambda^* = \overline{\Lambda^t}$. Soit $P_{\lambda s}(x, y)$ le coefficient d'indices x, y de $P_{\lambda s}$. Soit $\sigma \in G = S_n$:

$$\begin{aligned} P_{\lambda s}(\sigma x, \sigma y) &= (\Lambda\Lambda^*)(\sigma x, \sigma y) \\ &= \sum_{z \in X_s} \Lambda(\sigma x, z)\Lambda^*(z, \sigma y) \\ &= (\Lambda'\Lambda'^* x)(x, y) \end{aligned}$$

où Λ' est définie par : $\Lambda'(x, y) = \Lambda(\sigma x, y)$. Ainsi Λ et Λ' ont même lignes mais dans un ordre éventuellement différent, donc Λ' est aussi (la matrice d') une base orthonormée de V_λ^s : $P_{\lambda s} = \Lambda'\Lambda'^*$.
Finalement :

$$P_{\lambda s}(\sigma x, \sigma y) = P_{\lambda s}(x, y)$$

donc $P_{\lambda s}$ est zonale et il est aisé de voir qu'elle est sphérique.
A présent le théorème est facile à prouver :
($\Rightarrow$) : soit $F \in \mathcal{F}_\lambda$ et $x \in X_s$. La fonction F est harmonique donc le vecteur $\sum_{z \in X_s} F(x, z)z$ est dans V_λ^s et $f_\mathcal{B} \perp V_\lambda^s$ donc :

$$\langle \sum_{z \in X_s} F(x, z)z, f_\mathcal{B} \rangle = 0$$

ce qui signifie : $\sum_{y \in \mathcal{B}} F(x, y) = 0$.

($\Leftarrow$) :
nous avons :

$$\forall F \in \mathcal{F}_\lambda,\ \forall x \in \mathcal{B}, \quad \sum_{y \in \mathcal{B}} F(x, y) = 0$$

mais $P_{\lambda s}$ est harmonique, on en déduit :

$$\sum_{x,y \in \mathcal{B}} P_{\lambda s}(x, y) = 0$$

et ceci est $\| P_{\lambda s}.f_\mathcal{B} \|$ ainsi avons-nous bien : $f_\mathcal{B} \perp V_\lambda^s$. □

Donnons un exemple concret : plaçons-nous dans le cas $q = 3$, longueur n et $s = (s_0, s_1, s_2)$ avec $s_0, s_1, s_2 \geq 2$, nous avons la decomposition :

$$\mathbb{C}[X_s] = [n] \oplus 2[n-1, 1] \oplus 3[n-2, 2] \oplus [n-2, 1, 1] \oplus \dots$$

donc si nous cherchons des 2-designs nous aurons besoin de $2^2+3^2+1^2=14$ fonctions. Si l'on pose $C=\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ Ces fonctions sont :

$[n-1,1]$:
$-\ c/s_0+i/s_2$
$-\ c/s_0+f/s_1$
$-\ b/s_0+h/s_2$
$-\ b/s_0+e/s_1$

$[n-2,2]$:
$\frac{c(c-1)}{s_0(s_0-1)}-\frac{2ci}{s_0s_2}+\frac{i(i-1)}{s_2(s_2-1)}$
$\frac{2bc}{s_0(s_0-1)}-\frac{2bi}{s_0s_2}-\frac{2ch}{s_0s_2}+\frac{2hi}{s_2(s_2-1)}$
$\frac{b(b-1)}{s_0(s_0-1)}-\frac{2bh}{s_0s_2}+\frac{h(h-1)}{s_2(s_2-1)}$
$\frac{c(c-1)}{s_0(s_0-1)}-\frac{cf}{s_0s_1}-\frac{ci}{s_0s_2}+\frac{fi}{s_1s_2}$
$\frac{bc}{s_0(s_0-1)}-\frac{bf}{s_0s_1}-\frac{bi}{s_0s_2}-\frac{ce}{s_0s_1}-\frac{ch}{s_0s_2}+\frac{ei}{s_1s_2}+\frac{fh}{s_1s_2}$
$\frac{b(b-1)}{s_0(s_0-1)}-\frac{be}{s_0s_1}-\frac{bh}{s_0s_2}+\frac{eh}{s_1s_2}$
$\frac{c(c-1)}{s_0(s_0-1)}-\frac{2cf}{s_0s_1}+\frac{f(f-1)}{s_1(s_1-1)}$
$\frac{2bc}{s_0(s_0-1)}-\frac{2bf}{s_0s_1}-\frac{2ce}{s_0s_1}+\frac{2ef}{s_1(s_1-1)}$
$\frac{b(b-1)}{s_0(s_0-1)}-\frac{2be}{s_0s_1}+\frac{e(e-1)}{s_1(s_1-1)}$

$[n-2,1,1]$:
$\frac{bf}{s_0s_1}-\frac{bi}{s_0s_2}-\frac{ce}{s_0s_1}+\frac{ch}{s_0s_2}+\frac{ei}{s_1s_2}-\frac{fh}{s_1s_2}$

Troisième partie

Applications aux codes

Chapitre 5

Codes et designs

5.1 Rappels de théorie des codes

On désigne par $\mathbb{F}_q$ le corps fini à q éléments. Un *code* C de longueur n sur $\mathbb{F}_q$ est tout simplement un sous-ensemble de $\mathbb{F}_q^n$. Ses élements sont appelés les *mots* du code. Du point de vue de la correction d'erreurs (cf. Introduction) on peut donc assimiler un code à un *vocabulaire* formé des mots admissibles. Un *code linéaire* de longueur n sur $\mathbb{F}_q$ est un sous-espace vectoriel de $\mathbb{F}_q^n$. Le *poids de Hamming* $|u|$ d'un mot u est le nombre de ses coordonnées non nulles : $|u| = |\{i, u_i \neq 0\}|$. La *distance de Hamming* $d_H(u, v)$ de deux mots u et v est le nombre de coordonnées en lesquelles ces deux mots diffèrent : $d_H(u, v)|\{i, u_i \neq v_i\}|$. La *distance* $d(C)$ du code C est définie par :

$$d(C) = \min_{u,v \in C, u \neq v} d_H(u, v)$$

et si le code est linéaire c'est le plus petit poids de ses mots non nuls. Si n est la longueur, k la dimension et d la distance d'un code C on dit que C est un $[n, k, d]$ code.
Exemple : le code binaire

$$CR_n = \{\underbrace{(0, \ldots, 0)}_{n}, \underbrace{(1, \ldots, 1)}_{n}\}$$

est un $[n, 1, n]$ code appelé *code répétition.*
En longueur 8 le code binaire
$H_8 = \{(0,0,0,0,0,0,0,0), (1,0,0,0,1,1,0,1), (1,1,0,0,0,1,1,0), (0,1,0,0,1,0,1,1),$
$(0,1,1,0,0,1,0,1), (1,1,1,0,1,0,0,0), (1,0,1,0,0,0,1,1), (0,0,1,0,1,1,1,0),$
$(0,0,1,1,1,0,0,1), (1,0,1,1,0,1,0,0), (1,1,1,1,1,1,1,1), (0,1,1,1,0,0,1,0),$
$(0,1,0,1,1,1,0,0), (1,1,0,1,0,0,0,1), (1,0,0,1,1,0,1,0), (0,0,0,1,0,1,1,1)\}$

est un $[8, 4, 4]$ code appelé *code de Hamming étendu*.
Pour alléger l'expression d'un code C on donne parfois une *matrice génératrice* dont les lignes engendrent l'espace vectoriel C. Ainsi pour H_8 une matrice génératrice possible est :

$$M_{H_8} = \begin{pmatrix} 10001101 \\ 01001011 \\ 00101110 \\ 00010111 \end{pmatrix}.$$

Il est clair qu'en permutant les coordonnées des mots d'un code on obtient un code qui est essentiellement le même que le précédent. Aussi dit-on que deux codes sont *équivalents* si il existe une permutation de $\{1, \ldots, n\}$ qui les échange. Et l'on appelle *groupe de permutations* du code l'ensemble des permutations (des coordonnées) laissant invariant le code.
Dans le cas non binaire on peut aussi multiplier telle ou telle coordonnée par un élément de $\mathbb{F}_q$ non nul. On fait donc dans ce cas opérer $\mathbb{F}_q^* \rtimes S_n$.
Donnons à présent un exemple important de code binaire.

Théorème 24 *(Pless) A équivalence près il existe un unique code (non nécessairement linéaire) de cardinal 2^{12} et de distance 8. Ce code est appelé code de Golay étendu et est noté $\mathcal{G}_{24}$.*

Une matrice génératrice de ce code est :

$$M_{\mathcal{G}_{24}} = \begin{pmatrix} 100000000000101011100011 \\ 010000000000111110010010 \\ 001000000000110100101011 \\ 000100000000110001110110 \\ 000010000000110011011001 \\ 000001000000011001101101 \\ 000000100000001100110111 \\ 000000010000101101111000 \\ 000000001000010110111100 \\ 000000000100001011011110 \\ 000000000010101110001101 \\ 000000000001010111000111 \end{pmatrix}.$$

Enfin, voici un exemple de code non binaire :

Théorème 25 *Il existe un unique code ternaire de longueur 12 et de distance 6. Ce code est appelé code de Golay ternaire et est noté $\mathcal{G}_{12}$.*

Une matrice génératrice de ce code est :

$$M_{\mathcal{G}_{12}} = \begin{pmatrix} 100000011111 \\ 010000201221 \\ 001000210122 \\ 000100221012 \\ 000010222101 \\ 000001212210 \end{pmatrix}.$$

5.2 Polynômes énumérateurs de poids

Codes autoduaux

Soient $x, y \in \mathbb{F}_q^n$ on pose :

$$< x, y >= \sum_i x_i y_i$$

On appelle *dual* de C et on note $C^\perp$ l'ensemble $\{x \in \mathbb{F}_q^n, < x, u >= 0 \ \forall u \in C\}$. Un code est dit *autodual* si $C = C^\perp$. Dans ce cas la longueur n est nécessairement paire, C est linéaire et la dimension de C est $n/2$. Par ailleurs dans le cas binaire, si C est autodual on a pour tout mot u de C :

$$0 =< u, u >=< u, (1, \ldots, 1) >= |u| \ mod 2.$$

Ainsi le code contient-il le mot $(1, \ldots, 1)$; en outre tous les mots sont de poids pair : on dit que le code est *pair*. Lorsque tout les mots sont de poids multiple de 4 on dit que le code est *doublement pair*.
Pour simplifier, on dit d'un code qu'il est de *Type II* s'il est binaire autodual doublement pair et qu'il est de *type I* s'il est s'il est binaire autodual mais non doublement pair.
Les codes H_8, $\mathcal{G}_{24}$ et $\mathcal{G}_{12}$ sont des exemples de code autoduaux ; les deux premiers sont de Type II et le dernier est ternaire.
Dans le cadre de la théorie des codes correcteurs d'erreurs, les codes intéressants sont ceux dont la distance est grande (ils corrigent beaucoup d'erreur) mais qui contiennent également beaucoup de mots. Bien sûr il s'agit là de deux objectifs antagonistes - antagonisme que le théorème suivant précise :

Théorème 26 *(cf. [24]) Soit d la distance d'un code binaire autodual de longueur n. On a :*

$$d \leq 4\lfloor n/24 \rfloor + 4 \ si \ n \equiv 22 \bmod 24$$

$$d \leq 4\lfloor n/24 \rfloor + 6 \text{ sinon}$$

Soit d la distance d'un code binaire autodual doublement pair de longueur n. On a :

$$d \leq 4\lfloor n/24 \rfloor + 4$$

Si les inégalités précédentes sont en fait des égalités on dit que le code est *extrémal*, de type I ou II selon le cas. Exemples : H_8, $\mathcal{G}_{24}$ sont des codes extrémaux de type II.

Enumérateurs des poids d'un code

Soit $\{\alpha_0 = 0, \alpha_1, \ldots, \alpha_{q-1}\}$ les éléments de $\mathbb{F}_q$; rappelons que la composition d'un élément $x \in \mathbb{F}_q^n$ est, par définition, le q-uplet $s(x) = (s_0(x), \ldots, s_{q-1}(x))$ où $s_i(x) = |\{j = 1, \ldots, n, x_j = \alpha_i\}|$.

Définition 26 *On appelle énumérateur de poids complet d'un code C sur $\mathbb{F}_q$ le polynôme de $\mathbb{C}[X_0, \ldots, X_{q-1}]$ défini par :*

$$W_C^c(X_0, \ldots, X_{q-1}) = \sum_{u \in C} X_0^{s_0(x)} \ldots X_{q-1}^{s_{q-1}(x)}.$$

C'est donc un polynôme homogène de degré n et à q variables.
Exemple : pour le code de Golay ternaire on a :

$$W_{\mathcal{G}_{12}}^c(X_0, X_1, X_2) = X_0^{12} + 22X_0^6X_1^6 + 220X_0^6X_1^3X_2^3 + 22X_0^6X_2^6 + 220X_0^3X_1^6X_2^3$$

$$+220X_0^3X_1^3X_2^6 + X_1^{12} + 22X_1^6X_2^6 + X_2^{12}$$

Définition 27 *On appelle énumérateur de poids (de Hamming) d'un code C sur $\mathbb{F}_q$ le polynôme de $\mathbb{C}[X_0, X_1]$ défini par :*

$$W_C(X_0, X_1) = \sum_{u \in C} X_0^{n-|x|} X_1^{|x|}.$$

C'est donc un polynôme homogène de degré n, à 2 variables et obtenu en fait par restriction de W_C^c à $X_1 = \ldots = X_{q-1}$. Bien sûr dans le cas binaire les deux notions précédentes coïncident.
Exemple : pour le code répétition de longueur 2 on a :

$$W_{CR_2} = X_0^2 + X_1^2$$

pour le code de Hamming :

$$W_{H_8}(X_0, X_1) = X_0^8 + 14X_0^4X_1^4 + X_1^8$$

et pour le code de Golay binaire :

$$W_{\mathcal{G}_{24}} = X_0^{24} + 759X_0^{16}X_1^8 + 2576X_0^{12}X_1^{12} + 759X_0^8X_1^{16} + X_1^{24}.$$

Soit χ un caractère (non trivial) de $\mathbb{F}_q$, c'est-à-dire un homomorphisme

$$\chi : (\mathbb{F}_q, +) \to (\mathbb{C}^*, \times).$$

Notons M la matrice de terme général $M_{i,j} = \chi(\alpha_i\alpha_j)$ pour $i, j \neq 0$ et 1 si i ou j est égal à 0. Cette matrice agit sur les indéterminées $X_0, \ldots, X_{q-1}$:

$$M.X_k = \sum_{i=0}^{q-1} \chi(\alpha_k\alpha_i)X_i$$

et donc sur les polynômes de $\mathbb{C}[X_0, \ldots, X_{q-1}]$:

$$M.P(X_0, \ldots, X_{q-1}) = P(MX_0, \ldots, MX_{q-1}).$$

Les théorèmes qui suivent relient les énumérateurs des poids d'un code à ceux de son dual.

Théorème 27 *Formule de MacWilliams.*
Soit C un code linéaire sur $\mathbb{F}_q$ on a :

$$W_{C^\perp}^c = |C|^{-1}M.W_C^c$$

Corollaire *Soit C un code linéaire sur $\mathbb{F}_q$ on a :*

$$W_{C^\perp}(X_0, X_1) = |C|^{-1}W_C(X_0 + (q-1)X_1, X_0 - X_1)$$

Corollaire *Soit C un code binaire autodual, on a :*

$$W_C(X_0, X_1) = W_C(\frac{X_0 + X_1}{\sqrt{2}}, \frac{X_0 - X_1}{\sqrt{2}})$$

Comme par ailleurs un code binaire autodual est nécessairement pair, on en déduit que W_C est invariant pour la transformation $X_1 \mapsto -X_1$ associée à la matrice $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Ainsi W_C est-il invariant pour le groupe de transformation

$$\mathcal{C}_1 = < \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} > .$$

Notons $\mathbb{C}[X_0, X_1]^{\mathcal{C}_1}$ l'anneau des invariants de ce groupe. On a en fait le résultat suivant :

Théorème 28 *(Gleason)*

$$\mathbb{C}[X_0, X_1]^{\mathcal{C}_1} = \mathbb{C}[W_{H_8}, W_{CR_2}]$$

Dans le cas des codes autoduaux doublement pair W_C est invariant pour la transformation $X_1 \mapsto iX_1$ associée à la matrice $\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$. Posons

$$\mathcal{X}_1 =< \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} > .$$

on a alors :

Théorème 29

$$\mathbb{C}[X_0, X_1]^{\mathcal{X}_1} = \mathbb{C}[W_{H_8}, W_{\mathcal{G}_{24}}]$$

5.3 Designs classiques et codes binaires

Les codes s'avèrent être des objets particulièrement intéressant lorsque l'on cherche des designs ; en effet, comme le montre les théorèmes suivant, les "bons codes" ont tendance à contenir de "bons designs"...

Théorème 30 *(Assmus-Mattson)*
Si C est un code extrémal de type II et de longueur multiple de 24 alors les mots de C de même poids (non nul) forment un 5-design.

Remarque : les mots de $\mathbb{F}_2^n$ (de même poids w) s'identifient naturellement aux parties (à w éléments) d'un ensemble à n éléments ; c'est dans ce sens, mais par abus de langage, que l'on dit des mots qu'ils forment un design. Si l'on travaille sur $\mathbb{F}_q$ on dira que des mots forment un design (classique) si leur *support*, c'est-à-dire les mots binaires que l'on obtient après *blanchiment* et en évitant toute répétition, forment un design. Le théorème précédent apparaît alors comme un corollaire du théorème suivant :

Théorème 31 *(Assmus-Mattson)*
Soit C un $[n, k, d]$ code sur $\mathbb{F}_q$; son orthogonal $C^\perp$ est un $[n, n-k, e]$ code pour un certain e. Soit $t \leq d$ un entier. Enfin, si $q > 2$ soient v_0 le plus grand entier tel que

$$v_0 - \lfloor \frac{v_0 + q - 2}{q - 1} \rfloor < d$$

et w_0 le plus grand entier tel que

$$w_0 - \lfloor \frac{w_0 + q - 2}{q - 1} \rfloor < e$$

(si $q = 2$, on pose $v_0 = w_0 = n$).
Si le nombre de poids non nuls de $C^\perp$ inférieurs ou égaux à $n-t$ est inférieur ou égal à $d-t$ alors pour tout v tel que $d \leq v \leq v_0$ les supports des mots de C de poids v forment un t-design ; et de façon analogue, pour tout w tel que $e \leq w \leq w_0$ les supports des mots de $C^\perp$ de poids w forment un t-design.

Exemple : les 759 mots de poids 8 de $\mathcal{G}_{24}$ forment un 5-$(24, 8, 1)$ design.

5.4 Designs généralisés

A l'heure actuelle il n'existe pas encore de véritable théorème d'Assmus-Mattson pour les designs généralisés. Notons cependant que dans [26] l'auteur donne un analogue dans le cas de codes sur $\mathbb{Z}_4$ (et utilise pour cela l'énumérateur de poids harmonique défini par C. Bachoc, cf. 6.2). Cet analogue permet à son auteur de (re)trouver des 5-designs sur le $\mathbb{Z}_4$-code de Golay étendu.
Toutefois on peut parfois aisément déceler des designs généralisés grâce au théorème suivant, dont la démonstration est immédiate.

Théorème 32 *Si le groupe de permutation d'un code est t fois transitif alors l'ensemble des mots du code de même composition forme un t-design (généralisé).*

Exemple : le groupe de permutation du code de Golay ternaire $\mathcal{G}_{12}$ est 3 fois transitif donc l'ensemble des mots de composition fixée de ce code forme un 3-design.
On peut bien entendu se sevir aussi de l'algorithme vu dans la deuxième partie, paragraphe 4.6. Par exemple supposons que l'on cherche à savoir si les 7140 mots de composition $(24, 9, 3)$ du code S_{36} (Pless Symmetry Code

de longueur 36) forment un design. Une matrice génératrice du code est :

$$M_{S_{36}} = \begin{pmatrix}
100000000000000000011111111111111111 \\
010000000000000000201121222112221211 \\
001000000000000000210112122211222121 \\
000100000000000000211011212221122212 \\
000010000000000000221101121222112221 \\
000001000000000000212110112122211222 \\
000000100000000000221211011212221122 \\
000000010000000000222121101121222112 \\
000000001000000000222212110112122211 \\
000000000100000000212221211011212221 \\
000000000010000000211222121101121222 \\
000000000001000000221122212110112122 \\
000000000000100000222112221211011212 \\
000000000000010000222211222121101121 \\
000000000000001000212221122212110112 \\
000000000000000100221222112221211011 \\
000000000000000010212122211222121101 \\
000000000000000001211212221122212110
\end{pmatrix}$$

Posons $C = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$. Si nous cherchons des 2-designs on peut utiliser les fonctions vues en 4.6. Dans ce cas particulier on obtient :

$[n-1, 1]$:

$-\ c/24 + i/3$

$-\ c/24 + f/9$

$-\ b/24 + h/3$

$-\ b/24 + e/9$

$[n-2, 2]$:

$\frac{c(c-1)}{552} - \frac{ci}{36} + \frac{i(i-1)}{6}$

$\frac{bc}{276} - \frac{bi}{36} - \frac{ch}{36} + \frac{hi}{3}$

$\frac{b(b-1)}{552} - \frac{bh}{36} + \frac{h(h-1)}{6}$

$\frac{c(c-1)}{552} - \frac{cf}{216} - \frac{ci}{72} + \frac{fi}{27}$

$\frac{bc}{552} - \frac{bf}{216} - \frac{bi}{72} - \frac{ce}{216} - \frac{ch}{72} + \frac{ei}{27} + \frac{fh}{27}$

$\frac{b(b-1)}{552} - \frac{be}{216} - \frac{bh}{72} + \frac{eh}{27}$

$\frac{c(c-1)}{552} - \frac{cf}{108} + \frac{f(f-1)}{72}$

$\frac{bc}{276} - \frac{bf}{108} - \frac{ce}{108} + \frac{ef}{36}$

$\frac{b(b-1)}{552} - \frac{be}{108} + \frac{e(e-1)}{72}$

$[n-2,1,1]$:
$\frac{bf}{216} - \frac{bi}{72} - \frac{ce}{216} + \frac{ch}{72} + \frac{ei}{27} - \frac{fh}{27}$

On obtient 0 à chaque fois pour la somme du théorème vu au paragraphe 4.6. Ainsi ces mots forment-ils un 2-design (coloré fort à 3 couleurs). En revanche les supports de ces mots ne forment pas de 3-design (classique) donc la force de ce design est bien 2.

Chapitre 6

Enumérateurs harmoniques

6.1 Polynômes énumérateurs de poids multiple

Désormais nous nous plaçons dans le cas binaire.
Les énumérateurs de poids vus au chapitre précédent sont obtenus en sommant sur les mots d'un code ; ils nous renseignent sur leur répartition suivant leur poids ou leur composition. Il est en fait possible de définir des énumérateurs de poids tenant compte de la répartition des mots les uns par rapport aux autres. Plus précisément, soit $g \geq 1$ un entier et soit $x = (x_1, \ldots, x_g)$ un g-uplet d'éléments de $\mathbb{F}_2^n$; on peut aussi voir x comme une matrice de taille $g \times n$ ou encore , en considérant les colonnes de cette matrice, comme un n-uplet de mots de longueur g. Considérons à présent, pour tout $a \in \mathbb{F}_2^g$ la fonction n_a définie sur $(\mathbb{F}_2^n)^g$ par :

$$n_a(x) = |\{i = 1, \ldots, n, a = (x_{1,i}, x_{2,i}, \ldots, x_{g,i})\}|$$

autrement dit n_a compte combien de colonnes de la matrice x sont égales à a.

Définition 28 *On appelle $g^{ième}$ énumérateur des poids d'un code (binaire) C le polynôme de $\mathbb{C}[X_a, a \in \mathbb{F}_2^g]$ défini par :*

$$W_C^{(g)} = \sum_{u_1,\ldots,u_g \in C} \prod_{a \in \mathbb{F}_2^g} X_a^{n_a(u_1,\ldots,u_g)}.$$

Bien sûr, si $g = 1$ on a : $W_C^{(g)} = W_C$.

Remarque : Nous sommes dans le cas binaire, ainsi $q = 2$. Cela étant dit, on peut identifier $\mathbb{F}_2^g$ avec $\{0, 1, 2, 3, \ldots, 2^g - 1\}$ via la numération binaire :

$$0 = 0, 0, \ldots, 0,$$

$$1 = 1, 0, \ldots, 0,$$

$$2 = 0, 1, \ldots, 0,$$

$$3 = 1, 1, \ldots, 0,$$

etc. Grâce à ce procédé on peut remplacer n'importe quel élément x de $(\mathbb{F}_2^n)^g$ par un mot de longueur n sur l'alphabet $\{0, 1, 2, 3, \ldots, 2^g - 1\}$. Et l'on se rend alors facilement compte que le q-uplet $(n_a(x), a \in \mathbb{F}_2^g)$ n'est autre que la composition de ce mot ; et $W_C^{(g)}$ l'énumérateur des poids complet de C^g vu comme un code sur l'alphabet $\{0, 1, 2, 3, \ldots, 2^g - 1\}$. C'est pourquoi nous poserons désormais $q = 2^g$ et assimilerons $\mathbb{F}_2^g$ à $\mathcal{F}_q$.

Groupes de Clifford

Nous allons voir qu'il existe pour les énumérateurs de poids multiple des résultats d'invariance analogues à ceux obtenus pour l'énumérateur de Hamming. Définissons au préalable les groupes de Clifford réels et complexes et pour cela introduisons quelques notations :

- W_1 est la matrice de MacWilliams (notée M dans le chapitre précédent) :
$$W_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
- W_g est la matrice formée de 2^{g-1} blocs W_1 :
$$W_g = \begin{pmatrix} W_1 & 0 \\ 0 & \ddots \end{pmatrix}$$
- $AGl(g)$ est le groupe linéaire affine : $AGl(g) = \mathbb{F}_2^g \rtimes Gl(g, \mathbb{F}_2)$. Nous considérerons ce groupe comme un sous-groupe de $Gl(2^g, \mathbb{R})$ ou de $Gl(2^g, \mathbb{C})$ qui agit simplement par permutation des X_a.
- E est la matrice diagonale : $E = diag(1, i, 1, i, \ldots)$.
- Pour toute forme quadratique ϕ définie sur $\mathbb{F}_2^g$ à valeurs dans $\{0, 1\}$ et pour tout ε dans $\{0, 1\}$ soit $E_{\phi,\varepsilon}$ la matrice diagonale $diag((-1)^{\phi(a)+\varepsilon}), a \in \mathbb{F}_2^g$.

Définition 29 *On appelle $g^{ième}$ groupe de Clifford réel $\mathcal{C}_g$ le groupe engendré par $AGl(g)$, les matrices $E_{\phi,\varepsilon}$ et W_g.*
On appelle $g^{ième}$ groupe de Clifford complexe $\mathcal{X}_g$ le groupe engendré par $AGl(g)$, la matrice E et W_g.

B. Runge a démontré les résultats suivants :

Théorème 33 *L'anneau* $\mathbb{C}[X_a, a \in \mathbb{F}_2^g]^{\mathcal{C}_g}$ *des invariants de* $\mathcal{C}_g$ *est engendré par les* $g^{ième}$ *énumérateurs de poids des codes binaires autoduaux.*
L'anneau $\mathbb{C}[X_a, a \in \mathbb{F}_2^g]^{\mathcal{X}_g}$ *des invariants de* $\mathcal{X}_g$ *est engendré par les* $g^{ième}$ *énumérateurs de poids des codes binaires autoduaux doublement pairs.*

Une démonstration combinatoire de ce résultat a depuis été trouvée par G. Nebe, E. M. Rains et N. J. A. Sloane : cf. [22].

6.2 Enumérateurs de poids harmoniques

Soit C un code binaire de longueur n. Nous avons vu dans la première partie, paragraphe 2.5, les fonctions harmoniques associées au cas binaire. Soit donc $u \mapsto f_{k,v}(u) \stackrel{déf}{=} F_k(v,u)$ une fonction harmonique du sous-espace $W_{(n-k,k)}^{(n-k,k)}$ dans la décomposition :

$$L(X_{(n-k,k)}) = W_{(n-k,k)}^{(n-k,k)} \bigoplus_{l<k} W_{(n-l,l)}^{(n-k,k)}.$$

Une telle fonction est bien sûr unique à un facteur scalaire près et est définie sur $X_{(n-k,k)}$. Il est en fait possible d'étendre l'ensemble de définition de $f_{k,v}$ à tout $\mathbb{F}_2^n$ en posant pour tout $z \in \mathbb{F}_2^n$:

$$\widetilde{f_{k,v}}\,(z) = \sum_{y \in X_k, y \leq z} f_{k,v}(y)$$

la relation d'ordre sur les mots étant celle vue à la fin du paragraphe 1.4. On pose alors la :

Définition 30 *on appelle énumérateur harmonique du code* C *associé à la fonction* $f_{k,v}$ *le polynôme :*

$$W_{C,f_{k,v}}(X_0, X_1) = \sum_{u \in C} \widetilde{f_{k,v}}\,(u) X_0^{n-|u|} X_1^{|u|}.$$

En fait on peut montrer que $W_{C,f_{k,v}}(X_0, X_1)$ est toujours divisible par $X_0^k X_1^k$; posons $Z_{C,f_{k,v}}(X_0, X_1) = W_{C,f_{k,v}}/(X_0 X_1)^k$, dans [1] Christine Bachoc montre les résultats d'invariance suivants :

Théorème 34 *Si le code* C *est auto-dual, on a :*

$$M.Z_{C,f_{k,v}} = \mathrm{Det}^k\ M\ Z_{C,f_{k,v}} \quad \forall M \in \mathcal{C}_1$$

et si le code C *est auto-dual doublement pair :*

$$M.Z_{C,f_{k,v}} = \mathrm{Det}^k\ M\ Z_{C,f_{k,v}} \quad \forall M \in \mathcal{X}_1$$

Comme nous allons le voir il est en fait possible d'étendre ces résultats.
Soit toujours C un code binaire et soit à présent $u \mapsto f_{k,v}(u) \stackrel{déf}{=} f_k(u,v)$ la fonction harmonique vue à la définition 15.

Définition 31 *On appelle $g^{ième}$ énumérateur harmonique du code C associé à la fonction $f_{k,v}$ le polynôme de $\mathbb{C}[X_a, a \in \mathbb{F}_2^g]$ défini par :*

$$W^{(g)}_{C,f_{k,v}} = \sum_{u_1,\ldots,u_g \in C} f_{k,v}(u) \prod_{a \in \mathbb{F}_2^g} X_a^{n_a(u_1,\ldots,u_g)}.$$

On peut alors montrer(cf. paragraphe 6.4) que $W^{(g)}_{C,f_{k,v}}$ est toujours divisible par $\prod_{a\in\mathbb{F}_2^g} X_a^k$; posons $Z^{(g)}_{C,f_{k,v}} = W^{(g)}_{C,f_{k,v}} / \prod_{a\in\mathbb{F}_2^g} X_a^k$ on a les résultats d'invariance suivants :

Théorème 35 *Si le code C est auto-dual, on a :*

$$M.Z^{(g)}_{C,f_{k,v}} = \mathrm{Det}^k\ M\ Z^{(g)}_{C,f_{k,v}} \quad \forall M \in \mathcal{C}_g$$

et si le code C est auto-dual doublement pair :

$$M.Z^{(g)}_{C,f_{k,v}} = \mathrm{Det}^k\ M\ Z^{(g)}_{C,f_{k,v}} \quad \forall M \in \mathcal{X}_g$$

La preuve de ce théorème est donnée dans le paragraphe 6.4 ; elle utilise la notion d'*énumérateur de Jacobi* d'un code.
Outre son intérêt théorique ce théorème permet de construire explicitement des invariants pour $\mathbb{C}[X_a, a \in \mathbb{F}_2^g]$; cela peut être intéressant, notamment si l'on désire construire une base de $\mathbb{C}[X_a, a \in \mathbb{F}_2^g]^{\mathcal{C}_g}$ ou $\mathbb{C}[X_a, a \in \mathbb{F}_2^g]^{\mathcal{X}_g}$. En effet on ne sait pas généraliser les théorèmes 28 et 29 pour g quelconque. Dans le même ordre d'idée voir aussi la remarque finale.

6.3 Enumérateurs de Jacobi

Dans [21] M. Ozeki définit et étudie de nouveaux énumérateurs de poids qu'il appelle *polynôme de Jacobi*.

Définition 32 *Soit C un code de longueur n sur $\mathbb{F}_q$ et soit $v \in \mathbb{F}_q^n$. On appelle polynôme de Jacobi de C associé à v le polynôme :*

$$W_{C,v}(X_{0,0}, X_{0,1}, X_{1,0}, X_{1,1}) = \sum_{u\in C} X_{0,0}^{n-|u|-|v|+|u\cap v|} X_{0,1}^{|u|-|u\cap v|} X_{1,0}^{|v|-|u\cap v|} X_{1,1}^{|u\cap v|}$$

Il montre alors le théorème suivant :

Théorème 36 *Le polynôme de Jacobi vérifie une idntité de type MacWilliams :*

$$W_{C^\perp,v}(X_{0,0},X_{0,1},X_{1,0},X_{1,1}) =$$

$$\frac{1}{|C|}W_{C,v}(X_{0,0}+(q-1)X_{0,1},X_{0,0}-X_{0,1},X_{1,0}+(q-1)X_{1,1},X_{1,0}-X_{1,1})$$

Dans ce qui suit nous nous restreignons aux codes binaires auto-duaux ; nous généralisons la définition d'Ozeki puis nous établissons - entres autres résultats - l'analogue du théorème précédent dans ce cas.
Soient a,b deux éléments de $\mathbb{F}_2^g$, on peut voir (a,b) comme un élément de $\mathbb{F}_2^{2g}$ et (x,y) comme un élément de C^{2g} ; aussi poserons-nous :

$$n_{(a,b)}(x,y) = |\{i=1,\ldots,n, a=(x_{1,i},x_{2,i},\ldots,x_{g,i}), b=(y_{1,i},y_{2,i},\ldots,y_{g,i})\}|$$

Notons que la matrice $(n_{(a,b)}(x,y))_{a,b}$ correspond à la matrice $N(x,y)$ définie dans la première partie.

Définition 33 *Soit $v=(v_1,\ldots,v_g)\in(\mathbb{F}_2^n)^g$, on appelle $g^{ième}$ énumérateur de Jacobi de C associé à v le polynôme de $\mathbb{C}[X_{(a,b)},(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g]$ défini par :*

$$W_{C,v}^{(g)} = \sum_{u\in C^g}\prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(a,b)}(u,v)}.$$

Remarquons que les indéterminées $X_{(a,b)}$ s'identifient aux produits tensoriels $X_a\otimes X_b$ via l'isomorphisme :

$$\mathbb{C}[X_{(a,b)},(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g] = \mathbb{C}[X_a,a\in\mathbb{F}_2^g]\otimes\mathbb{C}[X_a,a\in\mathbb{F}_2^g]$$

il est donc possible d'étendre l'action des groupes de Clifford $\mathcal{C}_g$ et $\mathcal{X}_g$ aux indéterminées $X_{(a,b)}$ en posant : $M.X_{(a,b)} = M.X_a\otimes X_b \quad \forall b\in\mathbb{F}_2^g$. Rappelons (cf. première partie, 2.5) que Res est l'opérateur de *restriction* de $\mathbb{C}[X_{(a,b)},(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g]$ dans $\mathbb{C}[X_a,a\in\mathbb{F}_2^g]$ défini par $X_{(a,b)}\mapsto X_a$ pour tout b dans $\mathbb{F}_2^g$. Nous avons alors :

$$\text{Res } W_{C,v}^{(g)} = W_C^{(g)} \quad \forall v\in C^g.$$

et pour tout P dans $\mathbb{C}[X_{(a,b)},(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g]$:

$$M.\,\text{Res}\,P = \text{Res } M.P$$

ce qui permet de faire agir $\mathcal{C}_g$ et $\mathcal{X}_g$ sur le $g^{ième}$ énumérateur de Jacobi. Dans les trois propositions qui suivent nous montrons que si C est autodual alors $W_{C,v}^{(g)}$ est invariant sous l'action du groupe de Clifford. Notons que la preuve

de ce résultat figure également dans [5].

Proposition *Si C est auto-dual alors $W^{(g)}_{C,v}$ est W_g-invariant.*

Preuve :

dans cette preuve nous noterons :

$$W_{C_1,\ldots,C_g,v_1,\ldots,v_g} = \sum_{u_1\in C_1,\ldots,u_g\in C_g} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(a,b)}(u_1,\ldots,u_g,v_1,\ldots,v_g)}$$

une généralisation de l'énumérateur de Jacobi pour g codes de longueur n :

$$W_{C,\ldots,C,v_1,\ldots,v_g} = W^{(g)}_{C,v}.$$

Pour simplifier les notations nous poserons $u = (u_1,\ldots,u_g)$, $v = (v_1,\ldots,v_g)$ et pour i dans $1,\ldots,n$ nous considérerons l'élément de $\mathbb{F}_2^g$: $v^i = (v_{1,i},\ldots,v_{g,i})$. Avec l'aide de $\sum_{x\in C}(-1)^{<u_1,x>} = |C|$ si $u_1 \in C^\perp$ et 0 sinon, on calcule :

$$W_{C^\perp,C_2,\ldots,C_g,v} = \sum_{u_1\in C^\perp,u_2\in C_2,\ldots,u_g\in C_g} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(a,b)}(u_1,\ldots,u_g,v)}$$

$$= |C|^{-1} \sum_{x\in C,u_1\in\mathbb{F}_2^n,u_2\in C_2,\ldots,u_g\in C_g} (-1)^{<u_1,x>} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(a,b)}(u_1,\ldots,u_g,v)}$$

Maintenant, pour $x, u_2, \ldots, u_g$ fixés on a :

$$\sum_{u_1\in\mathbb{F}_2^n} (-1)^{<u_1,x>} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(a,b)}(u_1,\ldots,u_g,v)}$$

$$= \sum_{u_1\in\mathbb{F}_2^n} (\prod_{i=1}^n (-1)^{<u_{1,i},x_i>})(\prod_{i=1}^n X_{(u_{1,i},\ldots,u_{g,i},v^i)})$$

$$= \sum_{u_1\in\mathbb{F}_2^n} \prod_{i=1}^n (-1)^{<u_{1,i},x_i>} X_{(u_{1,i},\ldots,u_{g,i},v^i)}$$

et c'est exactement le développement de :

$$\prod_{i=1}^n ((-1)^{<0,x_i>} X_{(0,u_{2,i},\ldots,u_{g,i},v^i)} + (-1)^{<1,x_i>} X_{(1,u_{2,i},\ldots,u_{g,i},v^i)}).$$

Nous avons $(-1)^{<0,x_i>} = 1$, $(-1)^{<1,x_i>} = \begin{cases} -1 \; si \; x_i = 1 \\ 1 \; si \; x_i = 0 \end{cases}$ d'où :

$$(-1)^{<0,x_i>} X_{(0,u_{2,i},\ldots,u_{g,i},v^i)} + (-1)^{<1,x_i>} X_{(1,u_{2,i},\ldots,u_{g,i},v^i)}$$

$= (X_{(0,u_{2,i},\ldots,u_{g,i},v^i)}+X_{(1,u_{2,i},\ldots,u_{g,i},v^i)})^{n_0(x_i)}(X_{(0,u_{2,i},\ldots,u_{g,i},v^i)}-X_{(1,u_{2,i},\ldots,u_{g,i},v^i)})^{n_1(x_i)}$

où $n_0(x_i)$ (resp. $n_1(x_i)$) égale 1 si $x_i = 0$ (resp. $x_i = 1$) et 0 sinon. Finalement :

$$W_{C^\perp,C_2,\ldots,C_g,v} = |C|^{-1} \sum_{x\in C,u_2\in C_2,\ldots,u_g\in C_g} \prod_{(a',b)\in\mathbb{F}_2^{g-1}\times\mathbb{F}_2^g} (X_{(0,a',b)}+X_{(1,a',b)})^{n_{(0,a',b)}(x,u_2,\ldots,u_g,v)}$$

$$\times(X_{(0,a',b)} - X_{(1,a',b)})^{n_{(1,a',b)}(x,u_2,\ldots,u_g,v)}$$

$$= |C|^{-1}W_{C,C_2,\ldots,C_g,v}(X_{(0,0,\ldots,0)}+X_{(1,0,\ldots,0)}, X_{(0,0,\ldots,0)}-X_{(1,0,\ldots,0)}, X_{(0,1,\ldots,0)}+X_{(1,1,\ldots,0)}, \ldots)$$

et C est auto-dual, donc :

$$W_{C,v}^{(g)} = W_g.W_{C,v}^{(g)}$$

□

Proposition *Si C est auto-dual alors, pour tout M dans $AGl(g)$, $W_{C,v}^{(g)}$ est M-invariant.*

Preuve :
soit σ_M la transformation affine correspondant à la matrice M, de sorte que : $M.X_a = X_{\sigma_M a}$. Ainsi $M.X_{(a,b)} = X_{(\sigma_M a,b)}$ pour tout b dans $\mathbb{F}_2^g$; de plus, si l'on note $u^1,\ldots,u^n$ les colonnes de la matrice u (dont les lignes sont par définition les mots $u_1,\ldots,u_g$ de C) on définit alors l'action de σ_M sur u par : $\sigma_M u = (\sigma_M u^1,\ldots,\sigma_M u^n)$.
Calculons à présent :

$$M.W_{C,v}^{(g)} = \sum_{u\in C^g} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(\sigma_M a,b)}^{n_{(a,b)}(u,v)}$$

$$= \sum_{u\in C^g} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(\sigma_M^{-1}a,b)}(u,v)}$$

$$= \sum_{u\in C^g} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(a,b)}(\sigma_M u,v)}$$

$$= \sum_{u\in \sigma_M C^g} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(a,b)}(u,v)}$$

$$= \sum_{u\in C^g} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(a,b)}(u,v)} = W_{C,v}^{(g)}$$

car C est un espace vectoriel et contient le mot $(1, 1, \ldots, 1)$. □

Proposition *Si C est auto-dual alors $W_{C,v}^{(g)}$ est $E_{\phi,\varepsilon}$-invariant.*
Si C est auto-dual doublement pair alors $W_{C,v}^{(g)}$ est E-invariant.

Preuve :
dans le premier cas nous avons :

$$E_{\phi,\varepsilon}.W_{C,v}^{(g)} = \sum_{u\in C^g} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} ((-1)^{\phi(a)+\varepsilon} X_{(a,b)})^{n_{(a,b)}(u,v)}$$

$$= \sum_{u\in C^g} \prod_{a\in\mathbb{F}_2^g} (-1)^{(\phi(a)+\varepsilon)n_a(u)} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(a,b)}(u,v)}$$

$$= (-1)^{\varepsilon n} \sum_{u\in C^g} (-1)^{\sum_a \phi(a)n_a(u)} \prod_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g} X_{(a,b)}^{n_{(a,b)}(u,v)}$$

et n est pair donc $(-1)^{\varepsilon n} = 1$ et nous devons juste vérifier que $\sum_a \phi(a)n_a(u)$ est pair ; notons S la matrice symétrique associée à ϕ et telle que $\phi(a) = a^t Sa$:

$$\sum_a \phi(a)n_a(u) = \sum_{i=1}^{n} \phi(u_{1,i}, \ldots, u_{g,i})$$

$$= \sum_{i=1} \sum_{j,k=1}^{g} S_{j,k}u_{j,i}u_{k,i}$$

$$= \sum_{j,k=1}^{g} S_{j,k}|u_j \cap u_k|$$

$$= \sum_{j=1}^{g} S_{j,j}|u_j| + 2\sum_{j<k} S_{j,k}|u_j \cap u_k|$$

et C est auto-dual donc $|u_j|$ est toujours pair.
Dans le second cas la preuve est similaire : $|u_j|$ sera doublement-pair et $|u_j \cap u_k|$ sera pair car $< u_j, u_k >= 0$. □

6.4 Preuve du théorème 35

Soit $Q \in \mathbb{C}[x_1, \ldots, x_r]$ un polynôme à r indéterminées, on a vu dans la première partie comment lui associer un opérateur différentiel $Q(\partial)$: il suffit d'envoyer chaque monôme $x_1^{i_1} \ldots x_r^{i_r}$ sur $\frac{\partial^{i_1+\ldots+i_r}}{\partial x_1^{i_1} \ldots \partial x_r^{i_r}}$ (on envoie la constante 1

sur *identité*). Grâce au théorème 11 on a un lien entre les énumérateurs harmoniques et les énumérateurs de Jacobi :
Proposition

$$Z^{(g)}_{C,f_{k,v}} = \frac{W^{(g)}_{C,f_{k,v}}}{\prod_{a\in\mathbb{F}_2^g} X_a^k} = \text{Res } \text{Det}^k(\partial) W^{(g)}_{C,v}.$$

Or nous avons vu que pour tout M dans $\mathcal{C}_g$ ou $\mathcal{X}_g$ et pour tout P dans $\mathbb{C}[X_{(a,b)}, (a,b) \in \mathbb{F}_2^g \times \mathbb{F}_2^g]$:

$$M.\,\text{Res}\, P = \text{Res } M.P$$

Il s'agit donc de montrer l'invariance de $\text{Det}^k(\partial) W^{(g)}_{C,v}$. On déduit aisément des règles élémentaires de différentiation relatives au produit et à la composition de fonctions le lemme suivant :
Lemme *Soient $P, Q \in \mathbb{C}[x_1, \ldots, x_k]$ et $M \in \mathcal{M}_k(\mathbb{C})$, nous avons :*

$$Q(\partial)(M.P) = M.[(M^t.Q)(\partial)P].$$

Donc si P, Q sont M-invariants (respectivement pour l'action à gauche et à droite de M) alors $Q(\partial)P$ est également M-invariant (pour l'action à gauche de M).
Preuve :
par linéarité on peut supposer que P est un monôme $x_1^{i_1} \ldots x_k^{i_k}$. On peut également supposer que Q est un monôme, et en fait on va prouver la proposition en raisonnant sur son degré. Aussi commençons-nous avec $Q = x_j$.

$$Q(\partial)(M.P) = \frac{\partial}{\partial x_j}[(\sum_{l=1}^{k} M_{l,1}x_l)^{i_1} \ldots (\sum_{l=1}^{k} M_{l,k}x_l)^{i_k}]$$

$$= \sum_{r=1}^{k} M_{j,r} \times i_r \times (\sum_{l=1}^{k} M_{l,1}x_l)^{i_1} \ldots (\sum_{l=1}^{k} M_{l,r}x_l)^{i_r-1} \ldots (\sum_{l=1}^{k} M_{l,k}x_l)^{i_k}$$

$$= \sum_{r=1}^{k} M_{j,r}(M.\frac{\partial P}{\partial x_r})$$

$$= M.(\sum_{r} M_{j,r}\frac{\partial P}{\partial x_r})$$

$$= M.[(M^t.x_j)(\partial)P]$$

$$= M.[(M^t.Q)(\partial)P]$$

Maintenant, soit $R = x_h$ un troisième polynôme, on a :

$$\begin{aligned}(RQ)(\partial)(M.P) &= R(\partial)(Q(\partial)(M.P)) \\ &= R(\partial)(M.[(M^t.Q)(\partial)P]) \\ &= M.[(M^t.R)(\partial)(M^t.Q)(\partial)P] \\ &= M.[(M^t.(RQ))(\partial)P]\end{aligned}$$

et l'on conclut la preuve par récurrence. □

L'action (à droite) d'une matrice M sur les indéterminées $X_{(a,b)}$ est donnée par :

$M^t.X_{(a,b)} = \sum_{c\in\mathbb{F}_2^g} M_{a,c}X_{(c,b)} = (MX)_{a,b}$ où X est la matrice $(X_{(a,b)})_{(a,b)\in\mathbb{F}_2^g\times\mathbb{F}_2^g}$ et où MX désigne le produit matriciel habituel. Donc, si Q est le polynôme déterminant :

$$Q = \mathrm{Det}(X_{(a,b)})_{a,b\in\mathbb{F}_2^g}$$

nous avons q^2 indéterminées $X_{(a,b)}$ et : $M^t.Q = \mathrm{Det}\ MX = \mathrm{Det}\, M \times Q$. Comme en outre l'énumérateur de Jacobi est invariant sous l'action du groupe de Clifford, on en déduit le théorème 35. □

Remarques :

– la formule

$$\frac{W^{(g)}_{C,f_{k,v}}}{\prod_{a\in\mathbb{F}_2^g} X_a^k} = \mathrm{Res}\ \ \mathrm{Det}^k(\partial)W^{(g)}_{C,v}$$

prouve que le polynôme $\prod_{a\in\mathbb{F}_2^g} X_a^k$ divise le polynôme $W^{(g)}_{C,f_{k,v}}$; c'est une relation de divisibilité non triviale (comme on s'en convaincra en lisant dans [1] la preuve de ce résultat dans le cas particulier $g = 1$) ;

– outre qu'il permet de prouver le théorème 35, le lemme peut servir à construire directement de nouveaux invariants à partir d'anciens ; en effet voici un corollaire immédiat à ce lemme :
Corollaire *Si C_1 et C_2 sont deux codes auto-duaux alors $W^{(g)}_{C_1}(\partial)W^{(g)}_{C_2}$ est aussi $\mathcal{C}_g$-invariant.*
Par exemple :

$$W_{H_8}(\partial)W^4_{H_8} = \lambda W^3_{H_8} + \mu W_{\mathcal{G}_{24}} \qquad \lambda = 340907212800, \mu = 92484403200$$

ce qui montre que $W_{\mathcal{G}_{24}}$ peut en quelque sorte être déduit de W_{H_8}.

– T. Ibukiyama donne dans [14] des conditions nécessaires et suffisantes portant sur certains opérateurs différentiels pour que ceux-ci, appliqués à des formes modulaires donnent encore des formes modulaires.

Les séries thêta à coefficients sphériques d'un réseau obtenues à partir de certaines formes modulaires de Siegel (cf. [12]) apparaissent alors comme un simple cas particulier. Peut-être peut-on trouver pour les invariants des groupes de Clifford des résultats analogues à ceux de T. Ibukiyama ? En tout cas, le théorème 35 et la formule

$$\frac{W^{(g)}_{C,f_{k,v}}}{\prod_{a\in\mathbb{F}_2^g} X_a^k} = \text{Res}\ \ \text{Det}^k(\partial) W^{(g)}_{C,v}$$

sont un pas dans cette direction.

Bibliographie

[1] C. Bachoc, On harmonic weight enumerators of binary codes, *Designs, Codes and Cryptography*, 18 (1999), pp 11-28.

[2] A. Bonnecaze, E. Rains, P. Solé, 3-colored 5-designs and $\mathbb{Z}_4$-codes, *Journal of statistical planning and inference*, vol. 86 (2000), pp. 349-368.

[3] A. Bonnecaze, P. Solé, P. Udaya, Tricolore 3-designs in type III codes, *Discrete Math. 241 (2001)*, no. 1-3, 129–138.

[4] P. Camion, "Codes and Association Schemes" in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands : Elsevier, 1998.

[5] Y. Choie, S.T. Dougherty and Haesuk Kim, Complete joint weight enumerators and self-dual codes, preprint.

[6] J. H. Conway, N. J. A. Sloane, *Sphere packings, lattices and groups.* Grundlehren der mathematishen Wissenshaften, vol 290.

[7] P. Delsarte, "An algebraic approach to the association schemes of coding theory", *Philips Res. Repts. Suppl.,* vol. 10, 1973.

[8] P. Delsarte, "Hahn polynomials, discrete harmonics, and t-designs", *SIAM J. APPL. MATH.* vol. 34, No 1, 1978.

[9] C. F. Dunkl, *A Krawtchouk polynomial addition theorem and wreath products of symmetric groups* Ind. Univ. Math. Journal vol. 25, 1976, pp 335-358.

[10] W. Ebeling, *Lattices and codes*, Advanced Lectures in Mathematics, 1994.

[11] R. A. Fisher, *Contributions to Mathematical Statistics*, Wiley and Sons, New York, 1950.

[12] E. Freitag, Thetareihen mit harmonischen Koeffizienten zur Siegelschen Modulgruppe. *Math. Ann.* vol. 254 (1980), no. 1, 27–51.

[13] K. Hinkelmann, O. Kempthorne, *Design and analysis of experiments*, vol. 1, Wiley Series in probability and mathematical statistics, 1994.

[14] T. Ibukiyama, *On differential operators on automorphic forms and invariant pluri-harmonic polynomials*, Comment. Math. Univ. St. Paul. 48 (1999), no. 1, 103–118.

[15] G. James, A. Kerber, "The representation theory of the symmetric group."- Addison Wesley, 1981. - (Encyclopedia of Mathematics and its Appl./Addis.Wesley ; 16).

[16] J. H. Van Lint, *Introduction to coding theory*, Graduate Texts in Mathematics, Springer verlag, 1992.

[17] J. H. Van Lint, R. M. Wilson : *A course in combinatorics*, Cambridge University Press, 1992.

[18] I. G. Macdonald, "Symmetric functions and Hall polynomials", 2nd ed., Oxford University Press, Oxford, 1995.

[19] D. Masson, *Designs and representation of the symmetric group*, Designs, Codes and Cryptography, à paraître.

[20] D. Masson, *Harmonic enumerators of codes*, Journal of Algebraic Combinatorics, soumis.

[21] M. Ozeki, *On the notion of Jacobi polynomials for codes*, Math. Proc. Cambridge Philos. Soc. vol. 121, 1997, pp 15-30.

[22] G. Nebe, E. M. Rains, N. J. A. Sloane, The invariants of the Clifford groups, *Designs, Codes and Cryptography* 24 (2001), no. 1, 99–121

[23] B. Runge, Codes and Siegel modular forms, *Discrete Mathematics*, 148 (1996), pp 175-204.

[24] E. Rains, N. J. A. Sloane, Self-dual codes, *Handbook of Coding Theory*, V. Pless and W. C. Huffman editors, North Holland, Amsterdam, 1998

[25] B. Sagan, "The symmetric group : representations, combinatorial algorithms and symmetric functions." - Wadsworth and Brooks / Cole, 1991. - (Maths Series).

[26] K. Tanabe, An Assmus-Mattson theorem for Z_4-codes, *IEEE Trans. Inform. Theory* 46 (2000), no. 1, 48–53.

[27] H. Tarnanen, M. J. Aaltonen, and J.-M. Goethals, On the non binary Johnson scheme, *Europ. J. Combin.*, vol. 6 (1985), pp.279-285.

[28] A. Young, *Collected Papers*, University of Toronto, 1977.

[29] R. M. Wilson, "The exact bound in the Erdös-Ko-Rado theorem", *Combinatorica*, vol. 4, pp. 247-257, 1984.

Titre : Fonctions harmoniques, codes et designs

Résumé :

Cette thèse se compose de trois parties, chacune formée d'un chapitre de rappels et d'un chapitre contenant des "nouveautés". Dans la première partie, après des rappels sur la représentation du groupe symétrique, nous étudions certaines fonctions harmoniques associées à une représentation classique de S_n. Dans la deuxième partie nous donnons une caractérisation de certains designs généralisés dans le cadre des schémas d'association. Les fonctions harmoniques de la première partie nous permettent de déduire un algorithme pour tester si un ensemble donné est un design. Enfin dans la dernière partie nous définissons pour les codes binaires des énumérateurs de poids harmoniques ; dans le cas des codes autoduaux nous établissons des résultats d'invariance, notamment une identité de type MacWilliams.

Title : Harmonic functions, codes and designs

Abstract :

This thesis consists of three parts. In the first one, after some classical results about the representation of the symmetric group we study some harmonic functions attached to a representation of S_n. In the second part we characterize some generalized designs in the setting of association schemes. The harmonic functions computed in the first part allow us to derive an algorithm to test if a set is a design. In the last part we define some multiple harmonic enumerators of codes, associated to a binary code and to an harmonic function ; in the case of self-dual codes we prove for them a MacWilliams type equality.

Thèse de **Mathématiques Pures**

Mots-Clés : Représentation du groupe symétrique, Designs, Codes, Schémas d'association, Formule de MacWilliams, Tableaux.

Laboratoire A2X, Université Bordeaux I,
351 Cours de la Libération,
33405 TALENCE